THE OHIO STATE UNIVERSITY

Institutional Data

University Policy

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data.

Responsible Office

Office of the Chief Information Officer

POLICY

Issued: 10/18/2007
Revised: 08/15/2014

This policy specifies requirements for the protection of The Ohio State University's **institutional data** from unauthorized exposure or access and for relinquishment of such data when terminating relationship with the university. All institutional data must be assigned one of four data classification levels based on compliance, privacy, sensitivity, operational usage, and risk. Institutional data must be protected with security controls and access authorization mechanisms identified within The Ohio State University's Information Security Standard. The level of protection required for institutional data is based on the data classification level assigned to such data.

Institutional data includes, and is not limited to, information in paper, electronic, audio, and visual formats.

Purpose of the Policy

The purpose of this policy is to protect the university's institutional data while preserving the open, information-sharing mission of its academic culture. The university classifies institutional data in accordance with legal, regulatory, administrative, and contractual requirements; intellectual property and ethical considerations; strategic or proprietary value; and/or operational use.

Definitions

Term	Definition
Data stewards	Data stewards are designated university officials whose functional areas of responsibility include the creation or origination of institutional data. They have overall responsibility for managing and maintaining such data.
Data managers	Data managers are individuals assigned specific data management responsibilities by the data steward(s). They typically have operational level responsibility for the management of institutional data in their functional area.
Data custodians	Data custodians are individuals authorized by the data manager(s) or data steward(s) who have operational responsibility for the administration of the systems and devices that store, process, transmit, or provide access to institutional data.
Data users	Data users are individuals that have access to non-public institutional data to conduct university business and operations.
Institutional data	Institutional data is information created, collected, maintained, transmitted, or recorded by or for the university to conduct university business. It includes (a) data used for planning, managing, operating, controlling, or auditing university functions, operations, and mission; and (b) pursuant to the requirements as set forth in the Research Data policy, information created, collected, and maintained in the conduct or reporting of research at or under the authority of Ohio State, as applicable. Institutional data includes, but is not limited to, information in paper, electronic, audio, and visual formats.
Personal data	Personal data is information created, collected, maintained, transmitted, or recorded by university owned devices, media, or systems in accordance with the Responsible Use of University Computing and Network Resources policy that is personal in nature and not related to university business. Personal data includes, but is not limited to, information in paper, electronic, audio, and visual formats.

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data

Policy Details

I. Compliance.

A. Permission to access institutional data will be granted to eligible university community members for legitimate university purposes.

B. **Data users** who access institutional data must comply with all applicable: laws and regulations; university rules, policies, procedures, and standards; and contracts.

II. Data Classification.

A. All institutional data must be assigned one of four classifications based on compliance, privacy, sensitivity, operational usage, and risk. These classifications take into consideration legal, regulatory, administrative, and contractual requirements; intellectual property and ethical considerations; strategic or proprietary value; and/or operational use.

B. Based on the data classification level, authorization to access institutional data will vary and specific controls for access and protection will be applied in accordance with the Ohio State Information Security Standard. Proper classification is a prerequisite to enable compliance with legal and regulatory requirements, and university rules, policies, and standards. The four institutional data classifications are, from least to most restrictive:

1. Public. Public data is institutional data that is intended for public use and has no access or management restrictions.
2. Internal. Internal data is institutional data used to conduct university business and operations. It may only be accessed and managed by data users whose role, function, or assignment requires it. Unless otherwise indicated, internal is the default level for institutional data.
3. Private. Private data is institutional data classified as private due to legal, regulatory, administrative, or contractual requirements; intellectual property or ethical considerations; strategic or proprietary value; and/or other special governance of such data. Access to and management of private data requires authorization and is only granted to those data users as permitted under applicable law, regulation, contract, rule, policy, and/or role.
4. Restricted. Restricted data is institutional data that requires the highest level of protection due to legal, regulatory, administrative, contractual, rule, or policy requirements. Access to and management of restricted data is strictly limited as unauthorized use or disclosure could substantially or materially impact the university's mission, operations, reputation, finances, or result in potential identity theft.

C. Institutional data element assignments for the above listed data classifications and their permitted use in core university services and data user activities are specified in the following reference documents:

1. Institutional Data Element Classification Assignments. Maps institutional data elements to the appropriate data classification levels.
2. Permitted Data Usage By Activity. Identifies which classifications of institutional data are permitted for specific data user activities.
3. Permitted Data Usage By Service. Identifies which classifications of institutional data are permitted for specific core or hosted services.

III. Records Management.

A. Institutional data may reside in university records, be used to produce university records, or itself constitute university records.

B. University records need to be managed in accordance with approved records retention and disposition schedules consistent with University Archives records management policies and guidelines. Laws of the State of Ohio require that university records not be discarded or destroyed in advance of the authorized disposition date.

IV. Data Destruction.

A. To prevent unauthorized disclosure, institutional data must be properly disposed of using destruction methods that meet the legal, regulatory, and/or university record retention requirements for the data.

B. The Ohio State Information Security Standard provides guidance for the secure destruction of institutional data.

V. Public Records.

A. University records are generally "public records" which are available to the public under the State of Ohio's Public Records Law. Some records are protected by federal or state law or are otherwise exempt from disclosure.

B. Release of records in response to a public records request must be made in accordance with Ohio State's Public Records policy.

VI. Relinquishing Data.

All data users are required to relinquish institutional data upon termination or as required by changes in their role or relationship with the university, based on arrangements with senior management, **data steward** requirements, and/or the requirements set forth in the Ohio State Research Data policy.

PROCEDURE

Issued: 10/18/2007
Revised: 08/15/2014

I. University community members act in one or more specific roles when creating, collecting, maintaining, transmitting, accessing, or using institutional data and must understand and fulfill the responsibilities associated with their roles. Responsibilities for each role are listed in the Responsibilities section of this policy.

A. Data stewards. Designated university officials authorized to create or originate particular forms of institutional data and have overall responsibility for managing and maintaining such data. Data stewards also plan for future institutional data needs of the university.

B. **Data managers**. Authorized and assigned specific data management responsibilities by the data steward(s) and have operational level responsibility for the management of institutional data in their functional area. Data managers oversee the integrity of the data, as well as its accuracy and adherence to applicable university policies and standards. Data managers manage the access rights to the data they oversee and work with **data custodians** to implement controls in regard to the security and privacy of the data based on its classification.

C. Data custodians. Authorized by the data manager or data steward with operational responsibility for the administration of the systems and devices that store, process, transmit, or provide access to institutional data. Data custodians implement unit operating procedures and guidelines established by data stewards, data managers, and university policies and standards based on the data classification.

D. Data users. Authorized to use institutional data in conducting university business and operations.

II. The Institutional Data Classification Committee (IDCC) serves as the governance committee for institutional data classification.

A. IDCC membership will consist of data stewards or their designees, the chief information security officer or designee, the Wexner Medical Center data security director or designee, Executive Committee on Integrated Institutional Business Intelligence and Data Governance designee, University Senate designee, and other individuals at the IDCC's discretion.

B. The chief information officer or designee will chair and convene the IDCC on an as-needed basis.

C. The IDCC's responsibilities are described in the Responsibilities section of this policy.

III. All data users that access restricted institutional data must complete the Institutional Data Training course annually, at a minimum.

A. Additional training may be required for handling institutional data pursuant to legal, regulatory, administrative, or contractual requirements. University community members should consult their supervisor, unit management, or data manager regarding additional and ongoing training needs.

IV. Reporting a suspected loss, unauthorized access, or exposure of institutional data.

A. Any suspected loss, unauthorized access, or exposure of institutional data classified as private or restricted must be immediately reported.

1. OSU Wexner Medical Center data users should report suspected loss, unauthorized access, or exposures to the OSU Wexner Medical Center IT Help Desk (614-293-3861) and Privacy Office (issecurity@osumc.edu; privacyoffice@osumc.edu).

2. All other data users should report suspected loss, unauthorized access, or exposures to the Office of the Chief Information Officer (614-688-5650, security@osu.edu). Any suspected loss, unauthorized access, or exposure of protected health information must also be reported to the HIPAA privacy and IT security officer.

B. A suspected loss, unauthorized access, or exposure of institutional data classified as internal must be reported promptly to the appropriate unit management, unit human resource office, and/or to the Office of Human Resources for determination of any subsequent action or reporting required.

V. Units may implement additional unit operating procedures for institutional data within their areas of operational or administrative control.

A. If additional unit operating procedures for institutional data conflict with an element of this policy, they must be submitted to and approved by the IDCC prior to implementation. Submit such requests by emailing idcc@osu.edu.

B. Units must document and disseminate additional procedures or guidelines to their data users.

VI. Contact your unit's public records officer or the Office of University Compliance and Integrity for assistance regarding public records requests. For requests from media outlets, also contact the Office of University Communications.

VII. Data classification additions and modifications must be submitted to and approved by the IDCC. Submit such requests by emailing idcc@osu.edu.

VIII. Policy exception and waiver requests must be submitted to and approved by the IDCC. Submit such requests by emailing idcc@osu.edu.

IX. It is the responsibility of the data user to backup, save, manage, and maintain any **personal data**. Ohio State does not assume any liability and will not take responsibility for archiving, maintaining, managing, or granting access to any personal data.

X. Frequently Asked Questions (FAQs) regarding this policy are provided and should be referenced for additional clarification.

XI. Enforcement.

A. Data users who violate this policy may be denied access to university computing resources and may be subject to other penalties and disciplinary action, both within and outside of the university. Violations will be handled through university disciplinary procedures and/or civil/criminal prosecution applicable to the relevant data user under the circumstances.

B. The university may temporarily suspend or block access to an account and/or devices prior to the initiation or completion of such disciplinary procedures. The university may refer or be required to refer suspected violations of applicable law to appropriate law enforcement agencies.

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data

Responsibilities

Position or Office	Responsibilities
Institutional Data Classification Committee (IDCC)	1. Promote the importance of protecting and securing institutional data as an asset and establish standards and best practices. 2. Classify new or existing data elements in accordance with applicable legal, regulatory, administrative, and contractual requirements; intellectual property or ethical considerations; strategic or proprietary worth and/or university rules and policies. 3. Document and disseminate committee decisions and other relevant information to data stewards, data managers, data custodians, and data users. 4. Manage institutional data classification conflicts in regard to university rules, policies, standards, and unit operating procedures. 5. Oversee data stewards' responsibilities identified in this policy. 6. Respond to requests and questions submitted to idcc@osu.edu. 7. Consider and decide policy exceptions and/or waiver requests submitted for approval. 8. Consider and decide data classification addition or modification requests submitted for approval.
Data stewards	1. Understand and comply with university policies and standards for the access, use, disclosure, and protection of institutional data, including the Ohio State Information Security Standard. 2. Complete the Institutional Data Training course if restricted data is accessed. 3. Provide operational guidance and expertise regarding data access, use, and compliance with university rules, policies, standards and procedures as well as applicable legal, regulatory, administrative, and contractual requirements relating to data integrity, security, and confidentiality. 4. Publish and maintain data access procedures and approval processes for managing institutional data. 5. Facilitate appropriate institutional data access and relinquishment. 6. Oversee data manager responsibilities identified in this policy. 7. Serve or appoint a designee as a member of the IDCC. 8. Provide guidance for labelling electronic and physical media according to data classification as appropriate. 9. Remediate reports of unauthorized data access, misuse, or integrity issues. 10. Report suspected loss, unauthorized access, or exposure of institutional data.
Data managers	1. Understand and comply with university policies and standards for the access, use, disclosure, and protection of institutional data, including the Ohio State Information Security Standard. 2. Complete the Institutional Data Training course if restricted data is accessed. 3. Implement, manage, and maintain operating processes, procedures, and guidelines to comply with university rules and policies and applicable legal, regulatory, administrative, and contractual requirements relating to data integrity, security, and confidentiality. 4. Authorize institutional data access to data users who have a legitimate university purpose for the data and maintain records for data users with access. 5. Document and disseminate administrative and operational procedures to promote consistent and secure storage, processing, and transmission of institutional data. 6. Oversee data custodian responsibilities identified in this policy. 7. Document the source and provenance of institutional data and how it is stored, processed, and transmitted by those systems and data users with access. 8. Oversee that training in institutional data retention, handling, security, and destruction is provided to university community members responsible for managing the data. 9. Provide guidance for labelling electronic and physical media according to data classification. 10. Address reports of unauthorized data access, misuse, or integrity issues. 11. Report any suspected misuse, or integrity issues to the appropriate data manager or data steward for remediation. 12. Report suspected loss, unauthorized access, or exposure of institutional data.
Data custodians	1. Understand and comply with university policies and standards for the access, use, disclosure, and protection of institutional data, including the Ohio State Information Security Standard. 2. Complete the Institutional Data Training course if restricted data is accessed. 3. Maintain system and data security controls appropriate to the classification level of the institutional data in their custody. 4. Provision, de-provision, and administer data user access. 5. Provide for physical data storage, backup and recovery, operation, and availability of institutional data. 6. Verify that data users complete the necessary training as specified by the appropriate data manager. 7. Report any suspected data misuse or integrity issues to the appropriate data manager or data steward for

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data

Position or Office	Responsibilities
	remediation. 8. Report suspected loss, unauthorized access, or exposure of institutional data.
Data users	1. Understand and comply with university policies and standards for the access, use, disclosure, and protection of institutional data, including the Ohio State Information Security Standard. 2. Complete the Institutional Data Training course if restricted data is accessed. 3. Disseminate institutional data to others only when appropriately authorized. 4. Respect the confidentiality and privacy of all institutional data. 5. Report any suspected data misuse, or integrity issues to the appropriate data manager or data steward for remediation. 6. Report suspected loss, unauthorized access, or exposure of institutional data.
Office of the Chief Information Officer (OCIO)	1. Investigate suspected loss, unauthorized access, or exposure of institutional data notifications. 2. Consult with the Office of Human Resources on any subsequent actions or reporting required. 3. Notify the Office of University Compliance and Integrity of any suspected non-medical center breach that may contain protected health information within one business day. 4. Chair the IDCC. 5. Maintain the idcc@osu.edu email list. 6. Provide the Institutional Data Training course.
OSU Wexner Medical Center Data Security Team	1. Investigate suspected loss, unauthorized access, or exposure of institutional data notifications. 2. Consult with Wexner Medical Center Human Resources regarding any subsequent actions or reporting required.
Office of University Compliance and Integrity	1. Provide guidance on public record requests. 2. Provide guidance on addressing non-compliance with this policy.
Office of Legal Affairs	Provide advice and legal oversight regarding applicable laws and regulations protecting institutional data.
Office of Human Resources	Consult with units on corrective action and reporting.

Resources

Data Stewards for Institutional Data, go.osu.edu/idp-stewards
FAQ for Institutional Data policy, go.osu.edu/idp-faq
HIPAA Privacy and IT Security Officers, compliance.osu.edu/HIPAAprivacyITsecurity.pdf
Institutional Data Elements Classification Assignments, go.osu.edu/idp-elements
Institutional Data Training, go.osu.edu/idp-training
Information Technology Security policy, ocio.osu.edu/assets/Policies/ITSecurity.pdf
Information Security Standard, go.osu.edu/infosec-irmp
Ohio Public Records Law, codes.ohio.gov/orc/149.43
Permitted Data Usage by Activity, go.osu.edu/idp-activities
Permitted Data Usage by Service, go.osu.edu/idp-services
Public Records policy, compliance.osu.edu/PublicRecordsPolicy.pdf
Research Data policy, orc.osu.edu/files/2011/01/ResearchDataPolicy.pdf
Responsible Use of University Computing and Network Resources policy, ocio.osu.edu/policy/policies/responsible-use/

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions	Office of the Chief Information Officer, IT Risk Management	614-688-4357	ITPolicy@osu.edu
Corrective action	Office of Human Resources, Employee and Labor Relations	614-292-2800	ohrc@hr.osu.edu hr.osu.edu/elr
Institutional data (administrative only) use questions	Office of Academic Affairs, Institutional Research and Planning	614-292-1340	oaa.osu.edu/irp/home.php
Legal issues	Office of Legal Affairs	614-292-0611	legal.osu.edu
Media and other communications issues	Office of University Advancement, University Communications Media Relations	614-292-8285	ucom.osu.edu
Public records requests	Office of University Compliance and Integrity, Public Records Office	614-247-5833	PublicRecords@osu.edu compliance.osu.edu/public-records
Records management	University Libraries, University Archives	614-292-3271	library.osu.edu/projects-initiatives/osu-records-management
Report a suspected data loss, unauthorized access or exposure	Office of the Chief Information Officer, Enterprise Security	614-688-5650	security@osu.edu

History

Issued: 05/02/2007 (As Interim)
Revised: 10/18/2007
Revised: 08/15/2014