THE OHIO STATE UNIVERSITY

Institutional Data

University Policy

Applies to: Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and affiliated entities who are acting on behalf of the university

Responsible Office

Office of the Chief Information Officer

POLICY

Issued: 05/02/2007
Revised: 07/01/2021
Edited: 07/26/2021

The university's **institutional data** are significant assets that must be properly managed and protected by all members of the university community. Institutional data are assigned one of four data classification levels based on legal, regulatory, university, and contractual requirements; intellectual property and ethical considerations; strategic or proprietary value; operational use; and/or privacy. These classifications determine the control requirements that apply to reduce the risk of inappropriate access, use, disclosure, or generation of institutional data. **Data users** must follow the specific control requirements that apply for each data classification. Everyone this policy applies to has a responsibility to be a caretaker of institutional data.

Purpose of the Policy

To outline the appropriate use and protection of the university's institutional data while preserving the open, information-sharing culture of its academic mission.

Definitions

Term	Definition
Data Governance Council	Responsible for strategic guidance of the data governance program, prioritization of data governance projects and initiatives, and deciding issues that cannot be resolved at a lower level.
Data governance program	A framework of processes and tools established by the university that provides structure for formally managing the quality, integrity, and usability of institutional data.
Data users	Individuals who access, use, or generate institutional data to conduct university operations.
Data stewards	University officials who have been assigned to one of the stewardship roles under the data governance program. See the Data Governance webpage for details.
Institutional data	Information created, collected, maintained, transmitted, or recorded by or for the university to conduct university operations. It includes (a) research data and (b) data used for planning, managing, operating, controlling, or auditing university functions, operations, and mission, but does not include personally created data. Institutional data includes, but is not limited to, information in paper, electronic, audio, and visual formats.
Institutional data element	One piece of data which provides a specific representation of information. Classification of data is defined at the element level. The combination of data elements may result in a different classification than the individual elements. This is specified in the Institutional Data policy (IDP) Calculator and supporting documents.
Personally created data	Information created, collected, maintained, transmitted, or recorded that is not related to university business but is personal in nature.
Personally identifiable information	Information that can be used to distinguish or trace an individual's identity (such as their name, social security number, or biometric records) alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Research data	Primary records that are necessary for the reconstruction and evaluation of results of research and the events and processes leading to those results, regardless of the form of the media on which they may be recorded.
Unit	College or administrative unit

Applies to: Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and affiliated entities who are acting on behalf of the university

Policy Details

I. Compliance
   A. Permission to access, use, disclose, or generate institutional data will be authorized to data users only for legitimate university purposes. Authorization will be granted based on data user roles and compliance with university, contractual, and legal requirements.
   B. Permission to access, use, disclose, or generate **personally identifiable information** must also abide by the Ohio State Privacy Principles.
   C. Data users must comply with all applicable laws and regulations; university rules, policies, procedures, and standards; and contracts.
   D. In addition, **research data** must be managed in accordance with the Research Data policy.

II. Data Classification
   A. Proper classification of institutional data is a prerequisite to manage risk and enable compliance with legal and regulatory requirements, as well as university rules, policies, and standards. Unauthorized or improper use or disclosure of institutional data could substantially and/or materially impact the university's mission, operations, reputation, and finances, and could result in identity theft.
   B. All institutional data is assigned one of four classifications based on compliance, privacy, sensitivity, criticality, operational usage, and risk.
   C. The four institutional data classifications are, from least to most restrictive:
      1. Public (S1): Institutional data intended for public use that has no access or management restrictions.
      2. Internal (S2): Institutional data used to conduct university business and operations. Unless otherwise indicated, internal is the default level for institutional data.
      3. Private (S3): 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.
      4. Restricted (S4): Institutional data that requires the highest level of protection due to legal, regulatory, administrative, contractual, rule, or policy requirements.
   D. Specific controls will be applied based on the data classification level in accordance with the university Information Security Standard.
   E. **Institutional data element** assignments for the above listed data classifications and their permitted use are specified in the IDP Calculator and supporting documents.
   F. Requests to modify the classification of data element(s) must be submitted to and approved by the **Data Governance Council** or designee. Submit requests to datagovernance@osu.edu.

III. Records Management and Data Destruction
   A. Institutional data may reside in university records, be used to produce university records, or itself constitute university records.
   B. University records must be managed in accordance with approved records retention and disposition schedules consistent with the Records Management policy and guidelines. Ohio law requires that university records not be discarded nor destroyed prior to the expiration of the authorized retention period.
   C. To uphold Ohio State Privacy Principles, records must be disposed of in accordance with the Records Management policy and guidelines.
   D. The university Information Security Standard and the Records Management policy provide guidance for the secure destruction of institutional data.

IV. Public Records
   A. Although university records may be subject to disclosure pursuant to Ohio's Public Records Act, the underlying data maintained for university purposes must be protected according to its data classification.
   B. Public records requests must be handled in accordance with the Public Records policy.

Applies to: Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and affiliated entities who are acting on behalf of the university

V. Relinquishing Data
   A. All data users are required to relinquish institutional data upon the end of their university employment or as required by changes in their role or relationship with the university, arrangements with senior management, **data steward** requirements, contractual requirements, and/or university policy requirements. See the Research Data policy for pertinent additional details regarding research data.

PROCEDURE

Issued: 05/02/2007
Revised: 07/01/2021
Edited: 07/26/2021

I. Data Governance Council
   A. The Data Governance Council defines and publishes data classification assignments, governance processes, and data governance roles.
   B. The Data Governance Council is comprised of the following core members:
      1. Two co-chairs, one provided by the University Data Governance Program Office and the other provided by The Ohio State University Wexner Medical Center
      2. The university's chief information officer or designee
      3. The university's chief privacy officer
      4. Representatives of major constituency groups and/or major systems from the Office of Business and Finance; Office of Human Resources; University Registrar office; University Advancement; Office of Marketing and Communications; Enterprise for Research, Innovation and Knowledge: Office of Research; and Ohio State University Wexner Medical Center
      5. A member of the faculty, selected by the faculty council
   C. Additional Council members may be chosen by the core members.
   D. Further information on the Council and the university's **data governance program** can be found on the Data Governance webpage.

II. Training
   A. Data users with access to S4 data must complete university-approved institutional data training annually, at a minimum. All others must complete institutional data awareness annually.
   B. Additional training may be required for handling institutional data pursuant to legal, regulatory, administrative, or contractual requirements. University community members should consult their supervisor or data steward regarding additional and ongoing training needs.

III. Duty to Report
   A. All individuals to whom this policy applies must report a suspected unauthorized or inappropriate access, use, disclosure, or generation of institutional data immediately upon discovery to their local IT help desk or security responders as set forth in the Information Security Incident Response Management policy.

IV. Additional Requirements and Operating Procedures
   A. The university Research Data policy describes the proper access, use, disclosure, and generation of research data.
   B. The university Protected Health Information and HIPAA policy provides the mechanisms to comply with the Health Information Portability Accountability Act (HIPAA) and corresponding regulations.
   C. The Ohio State Privacy Principles describe the university's commitment to privacy, including providing notice, accessing and requesting changes to personal information, providing and honoring choices, and investigating reports of privacy violations.
   D. **Units** may implement additional unit operating procedures or guidelines for institutional data.

Applies to: Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and affiliated entities who are acting on behalf of the university

1. If units wish to implement additional unit operating procedures that conflict with or differ from any element of this policy, they must submit such proposed procedures to the Data Governance Council for review and approval prior to implementation. Submit review requests to datagovernance@osu.edu.
2. Any additional procedures or guidelines created by a unit must be documented and disseminated to its data users.

V. Personally Created Data
   A. It is the responsibility of the data user to back up, save, manage, and maintain any **personally created data**.
   B. The university does not assume any liability and will not take responsibility for archiving, maintaining, managing, or granting access to any personally created data as it is not considered institutional data.

VI. Policy Exceptions
   A. Policy exception requests must be submitted to and approved by the Data Governance Council or designee. Submit requests to datagovernance@osu.edu.

VII. Policy Violations
   A. Data users who violate this policy may be denied access to university computing resources. The university may enforce corrective or disciplinary action, up to and including termination or dismissal, in accordance with applicable policies or rules for violations of this policy.
   B. The university may temporarily suspend or block access to university computing resources prior to the initiation or completion of disciplinary procedures.
   C. The university may refer or be required to refer suspected violations of applicable law to appropriate law enforcement agencies.
   D. Policy violators may be subject to civil litigation or criminal prosecution depending on the circumstances.

Responsibilities

Position or Office	Responsibilities
All individuals to whom this policy applies	1. Properly manage and protect institutional data as set forth in the policy. 2. Report suspected unauthorized or inappropriate access, use, disclosure, or generation of institutional data immediately as set forth in the policy. 3. Complete required training or awareness annually as set forth in the policy.
Data Governance Council	1. Responsible for strategic guidance of data governance program, prioritization of data governance projects and initiatives, and deciding issues that cannot be resolved at a lower level. 2. Define and publish data classification assignments, governance processes, and data governance roles. 3. Review requests to modify the classification of data elements. 4. Review requests to implement unit operating procedures that conflict with or differ from any element of this policy. 5. Review policy exception requests.
Data users	1. Follow specific control requirements that apply for each data classification. 2. Comply with all applicable laws and regulations; university rules, policies, procedures, and standards; and contracts. 3. Relinquish institutional data upon end of university employment or as otherwise required as described in the policy. 4. Complete required training or awareness annually as set forth in the policy. 5. Back up, save, manage, and maintain any personally created data.
Unit	1. Document and disseminate any additional unit procedures or guidelines to unit data users. 2. Obtain prior approval from Data Governance Council for any unit operating procedures that conflict with or differ from any element of this policy.

Applies to: Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and affiliated entities who are acting on behalf of the university

Resources

Governance Documents

- General Records Retention Schedule, go.osu.edu/retention-schedules
- Information Security Incident Response Management Process policy, go.osu.edu/infosec-isirmp
- Information Security Standard, go.osu.edu/infosec-iss
- Information Technology Security policy, go.osu.edu/itsp
- Ohio Public Records Law, codes.ohio.gov/orc/149.43
- Protected Health Information and HIPAA policy, go.osu.edu/phi-hipaa-policy
- Public Records policy, compliance.osu.edu/PublicRecordsPolicy.pdf
- Records Management policy, go.osu.edu/records
- Research Data policy, go.osu.edu/researchdatapolicy
- Responsible Use of University Computing and Network Resources policy, go.osu.edu/responsible-use

Training and Awareness

- Institutional Data Awareness, cybersecurity.osu.edu/IDP_Awareness
- Institutional Data Training, go.osu.edu/idp-training
- OSUWMC HIPAA and Institutional Data Compliance Training, go.osu.edu/idp-training

Additional Guidance

- Cybersecurity4You, cybersecurity4you.osu.edu
- Data Governance Program, go.osu.edu/datagovernance
- Data Management Plans, guides.osu.edu/IntroDataManagement
- Data Stewards for Institutional Data, go.osu.edu/idp-stewards
- FAQs 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
- Ohio State Privacy Principles, privacy.osu.edu
- OSU Records Management, go.osu.edu/records

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions	Office of the Chief Information Officer, Security and Privacy Governance	614-688-4357	riskmgmt@osu.edu
Corrective action	Office of Human Resources, HR Connection	614-247-6947	HRConnection@osu.edu
Legal issues	Office of Legal Affairs	614-292-0611	legal.osu.edu
Media and other communications issues	Office of Marketing and Communications	614-292-9681	ucom.osu.edu
Public records requests	Office of University Compliance and Integrity, Public Records	614-247-5833	PublicRecords@osu.edu compliance.osu.edu/public-records
Records management questions	University Libraries, University Archives	614-292-4092	lib-records@osu.edu go.osu.edu/records

Applies to: Faculty, staff, students, student employees, contractors, volunteers, visitors, sponsored guests of units, and affiliated entities who are acting on behalf of the university

Report a suspected data loss, unauthorized access or exposure	Local Help Desk Or 8-Help Office of the Chief Information, Officer, Enterprise Security Operations OSU Wexner Medical Center, IT Help Desk	Local # 614-688-5650 614-293-4357	Local Help Desk security@osu.edu issecurity@osumc.edu
Data Governance Council questions	Office of the Chief Information Officer, Data and Analytics	614-688-3347	DataGovernance@osu.edu

History

Issued:	05/02/2007	As Interim
Revised:	10/18/2007	
Revised:	08/15/2014	
Reviewed:	05/17/2018	
Revised:	07/01/2021	Reflects revision approved by President's Cabinet and subsequent edit to reference the newly structured Office of Marketing and Communications and Enterprise for Research, Innovation and Knowledge: Office of Research
Edited:	07/26/2021	