



Ohio Administrative Code

Rule 3341-7-15 Research Data Protection, Security, and Ownership.

Effective: [October 22, 2026](#)

(A) Policy statement and purpose

(1) Statement of institutional authority

Bowling Green State University (BGSU) is committed to ensuring responsible stewardship, protection, and management of Research Data (as defined in this policy). BGSU asserts institutional ownership of Research Data generated under university research activities and establishes obligations for proper collection, management, security, storage, access, sharing, confidentiality, retention.

This policy is intended to promote compliance with:

- (a) Federal and state data protection laws;
- (b) Sponsor and funding agency requirements;
- (c) University research integrity and security standards; and
- (d) Requirements for transparency, reproducibility, and responsible research.

(2) Purpose of this policy

The purpose of this policy is to:

- (a) Define ownership, responsibilities, access rights, and security expectations for Research Data;
- (b) Safeguard the confidentiality, integrity, availability, and long-term stewardship of Research Data;
- (c) Support compliance with federal, state, and contractual requirements;
- (d) Promote ethical and transparent research practices; and
- (e) Establish high-level obligations for collection, storage, retention, archiving, sharing, and preservation.

Procedures, detailed workflows, and specific technical requirements will be maintained separately by the Division of Research.

(3) Governing principles



3341-7-15

2

- (a) Integrity and Accuracy - Research Data must be collected, stored, and maintained in a manner that supports transparency, reproducibility, and verification of research findings.
- (b) Security and Protection - All Research Data must be protected from unauthorized access, disclosure, alteration, or destruction.
- (c) Compliance - All BGSU researchers must comply with applicable laws, sponsor terms, intellectual property requirements, data-use agreements, and University standards.
- (d) Stewardship - Principal Investigators are the primary stewards of Research Data but must manage data in accordance with University oversight and ownership.

(B) Policy definitions

(1) Research

A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge (45 CFR 46.102(d)).

(2) Research data

Any records, materials, or results needed to replicate, validate, or verify research findings.

(3) Research record

Documentation that describes, explains, or supports Research Data.

(4) Principal Investigator (PI)

Individual responsible for the intellectual direction and administrative oversight of a project and managing Research Data stewardship.

(5) Metadata

Information required to interpret or reproduce Research Data.

(C) Policy scope

(1) Research data ownership



3341-7-15

3

Institutional ownership ensures BGSU's ability to fulfill legal and regulatory obligations, respond to audits or investigations, protect Research Data if a PI leaves the University, and preserve research continuity. Researchers may keep a copy of Research Data as permitted but original datasets are University property.

BGSU asserts institutional ownership of Research Data generated from:

- (a) University-administered funding, including all forms of sponsored projects such as grants, contracts, cooperative agreements, subawards, fellowships, internally funded programs, and any other externally or internally supported research, scholarly, or creative activity administered through the University.
- (b) Under any institutional agreement, memorandum of understanding, data use agreement, material transfer agreement, collaboration agreement, or other formal partnership entered into by the University or its personnel acting on behalf of the University, unless the agreement explicitly assigns ownership elsewhere.
- (c) Research conducted by University personnel, including faculty and staff when acting within the scope of their employment, and students when working on projects that fall under this policy (e.g., projects funded, supervised, or otherwise supported by the University).
- (d) Research using University resources, including equipment, facilities, core facilities, or infrastructure, as well as research conducted by visiting researchers, external collaborators, contractors, or other non BGSU personnel when such research relies on University owned or University managed facilities or infrastructure.

(2) Research data protection and security

Researchers must:

- (a) Implement appropriate administrative, physical, and technical safeguards
- (b) Protect confidential, limited access, or restricted data;
- (c) Comply with data-use agreements, IRB/IACUC/IBC requirements, and sponsor mandates;
- (d) Prevent unauthorized access or disclosure;



3341-7-15

4

- (e) Utilize standardized metadata schemas (such as the FAIR principles- Findable, Accessible, Interoperable, and Reusable) to support enterprise data cataloging and long-term archiving; and
- (f) Ensure Research Data is stored using approved University systems.

Research data protection and security must align with BGSU ITS Data Protection Standards.

Research covered by this policy may be subject to additional review and approval or disapproval by officials of BGSU.

Inappropriate attempts to influence the compliance process, individual compliance members, or Research Integrity staff will be reported to the Vice President for Research. The Vice President for Research will investigate and appropriately respond to these concerns and has the authority to limit or remove an Investigator's privilege to conduct research after due process.

(3) Research data retention

Minimum retention:

- (a) Seven (7) years after final publication or project completion, whichever occurs later.
- (b) Longer if required by sponsors, regulations, contracts, litigation holds, or compliance reviews.

Retention must follow University records management requirements.

If Research Data is not actively being securely preserved at the end of its required retention lifecycle, it must be purged or securely destroyed in accordance with BGSU Records Management requirements and approved data destruction practices to prevent unauthorized access and mitigate the risk of data breaches.

(4) University access to research data

BGSU may access research data for;

- (a) Regulatory or compliance investigations;
- (b) Grant or sponsor audits;



3341-7-15

5

- (c) Research misconduct proceedings;
- (d) Public records obligations, when applicable; and
- (e) Ensuring continuity when a PI leaves.

PIs must provide access to Research Data upon reasonable request.

Collaborators have reasonable access to Research Data required to continue their work.

(5) Leaving the university

When a PI or research personnel leave BGSU:

- (a) Original Research Data must remain with BGSU;
- (b) A copy may be taken with permission (unless restricted by law or contract);
- (c) Transfers of original Research Data require formal University approval. Departing researchers must follow BGSU's separation procedures; and
- (d) The Research Integrity Director may assume custody of Research Data to ensure compliance or continuity.

(6) Research data sharing and archiving

Researchers are encouraged to share Research Data when appropriate, following:

- (a) Ethical standards;
- (b) Legal/privacy protections;
- (c) Sponsor/public access requirements; and
- (d) Intellectual property considerations.

Limited access or restricted data may only be shared with proper approvals and agreements (e.g., Data-Use Agreements).

(7) Review by institution

Research Data management activities may be subject to additional review by BGSU officials; however:



3341-7-15

6

No BGSU official may authorize the transfer, release, or destruction of Research Data that violates this policy, federal regulations, sponsor terms, or contractual obligations.

(8) Use of procedures

Research Integrity will maintain procedures that address:

- (a) Secure storage;
- (b) Access management;
- (c) Data collection practices;
- (d) Data retention schedules;
- (e) Archiving and public access procedures;
- (f) Data sharing and transfer requirements;
- (g) Transfer and departure workflows; and
- (h) Data breach and incident reporting.

Procedures will be published separately and updated as needed.

(9) Compliance

Failure to comply with this policy may result in:

- (a) Suspension of research privileges;
- (b) Corrective action requirements;
- (c) Disciplinary action under University policies;
- (d) Reporting to funding agencies or regulatory bodies; and
- (e) Required audits or reviews.

Misconduct involving falsification, fabrication, or destruction of Research Data will follow the University's research misconduct procedures.

(D) Policy provisions

(1) Responsible office



3341-7-15

7

The Division of Research is responsible for the oversight and implementation of this policy.

(2) Implementation of policy

Who	Task
Vice president for research	Oversight; enforcement; investigation of concerns
Division of research/research integrity	Maintain procedures; provide training; coordinate compliance; ensure secure data management systems
Principal investigators	Steward research data; ensure proper collection, access, retention, security, sharing compliance, and adherence to all applicable requirements.

(E) Related university policies

- (1) 3341-7-5 - Research and Sponsored Project Integrity and Misconduct
- (2) 3341-7-7 - Protection of Human Subjects
- (3) 3341-7-8 - Protection of Vertebrate Animals
- (4) 3341-7-11 - Export Control
- (5) 3341-7-14 - Material Transfer, Data Use, and Confidentiality

(F) Related government policies and guidance

- (1) Federal data sharing and retention guidelines
- (2) Sponsor-specific data management requirements
- (3) Privacy and confidentiality laws (e.g., FERPA and HIPAA where applicable)
- (4) Records retention and destruction regulations
- (5) General Data Protection Regulation (GDPR)
- (6) The Personal Information Protection Law (PIPL)