Data Policy

Effective Date:	April 7, 2020
Revised Date:	January 14, 2026
Department:	Information Technology
Former Title:	Data Governance Policy
Administration:	Chief Information Security Officer

PURPOSE

This Data Policy ensures that information is handled securely, respectfully, and lawfully at every stage — from collection to disposal. It guides how the Butler University protects the privacy of individuals, maintains trust with stakeholders, and ensures that data is used only in ways that support its mission. By following this policy, the organization reduces risks, remains compliant with applicable laws, and enables everyone to make informed, responsible decisions about data.

POLICY STATEMENT

1. Data Classification Categories
    a. Public
        i. Information intended for broad distribution, such as published research abstracts, course catalogs, and marketing materials. Public information is not restricted by local, state, national or international statute regarding its use of disclosure.
    b. Internal
        i. Information for University use only, such as internal reports, meeting notes, and directory information. This data may be accessed by eligible employees and designated appointees of the university for purposes of university business.
    c. Restricted

i. Sensitive information that requires controlled access, including student records protected by FERPA, personnel files, and donor records. Because of legal, ethical, or other constraints, this data may not be accessed without specific authorization

d. Critical
   i. Highly sensitive data where unauthorized access could cause significant harm. This data includes but is not limited to national identifier (such as Social Security numbers), financial account details, or protected health information (PHI). Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, damage to university reputation, and/or unauthorized access.

2. Roles and Responsibilities
   a. Chief Information Security Officer (CISO)
      i. Leads the University's information security program and ensures compliance with relevant laws, regulations, and policies.
      ii. Develops and maintains data security standards, guidelines, and training.
      iii. Oversees incident response for data breaches or security events involving University data.
   b. General Counsel
      i. Provides legal guidance on data-related issues, including privacy, intellectual property, records retention, and regulatory compliance (e.g., FERPA, HIPAA, GDPR).
      ii. Reviews and advises on contracts, data-sharing agreements, and vendor arrangements to ensure legal protections for University data.
      iii. Supports the CISO and Data Owners in responding to incidents that have legal or regulatory implications.
      iv. Advises on risk mitigation strategies and ensures that University actions align with applicable laws and legal obligations.
   c. Data Stewards
      i. Designated by an Executive Vice President, typically senior administrators or designated leaders responsible for specific data domains (e.g., student records, HR data, financial data).
      ii. Define appropriate uses for their data.
      iii. Establish and enforce data quality standards, ensuring accuracy, completeness, and timeliness.
   d. End Users (Faculty, Staff, Students, Affiliates, Contractors)
      i. Access and use University data only for legitimate academic, operational, research, or administrative purposes.
      ii. Follow data handling, storage, and sharing requirements for their role and data classification.

iii. Protect login credentials and secure devices to prevent unauthorized access.
iv. Report suspected data breaches, misuse, or errors promptly to the CISO (security@butler.edu)

e. Third-Party Vendors and Contractors
i. Must comply with Butler University's Data Policy and applicable contractual data protection requirements.
ii. Use University data only for purposes approved in their contract or agreement.
iii. Notify the University immediately of any incident involving University data.
iv. Implement security measures that meet or exceed University standards, subject to review by the CISO or General Counsel when appropriate.

3. Collecting and Using Data
   a. Collect only the data that is necessary for the stated academic, operational, or research purpose.
   b. Clearly communicate, when applicable, why the data is being collected and how it will be used.
   c. Use data strictly for the purpose for which it was collected; secondary uses must be approved by the appropriate University authority.

4. Storing and Retaining Data
   a. Store institutional data only in approved, secure systems or locations managed or sanctioned by Butler University.
   b. Data with a classification other than Public may not be stored on personal devices.
   c. Data with a classification of Restricted or Critical may not be permanently stored on workstations, laptops, or other Butler-owned computing devices.
   d. Retain data only for as long as it serves a valid academic, business, or legal purpose, in accordance with the University's information retention schedule.
   e. Dispose of data securely, whether by shredding physical documents or using approved digital deletion methods.

5. Accessing and Sharing Data
   a. Access data only if it is necessary for your role or authorized responsibilities.
   b. Only data classified as Public may be shared outside of the university, unless explicitly authorized by the Data Steward, the General Counsel, or the Chief Information Security Officer.
   c. Confidential information, including but not necessarily limited to, Personally Identifiable Information (PII) as defined by Indiana Code, Protected Health

Information as defined by the Health Information Portability and Accountability Act (HIPAA), or Student Information as defined by the Family Educational Rights and Privacy Act (FERPA) may only be shared internally with authorized individuals who require access to carry out job responsibilities.

6. Data Accuracy and Quality
    a. Upon discovery of incorrect, incomplete, or outdated data, work with the appropriate department or Data Steward to make corrections quickly.
    b. Whenever possible, obtain data from authoritative University systems or designated records offices (e.g., Registrar, Human Resources, Finance).
    c. Avoid data duplication and refrain from creating separate "shadow" versions of official datasets unless absolutely necessary and approved.

7. Data Access
    a. Butler University will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the relevant Data Steward to have an appropriate access level. Data access will be conducted in accordance with the policies established by the Butler University Information Technology department.

8. Data Integration with Third-Party Technology
    a. Any/all institutional data integration with third-party technology, tools, contractors, or affiliates must be approved by the Chief Information Security Officer.

9. Data Loss Prevention (DLP)
    a. Butler University will employ a DLP tool to monitor digital assets containing sensitive information and ensure handling in accordance with this policy.
    b. If restricted or critical data are transferred from the application server file space to another computer (including via email), they must be conveyed using an encrypted method such that no unauthorized person can view it or intercept it.

10. Data Disclosure Requests
    a. Recipients of disclosure requests should seek guidance from the Chief Information Security Officer or General Counsel.

DEFINITIONS

1. Institutional data**:**

a. Data in any form, location, or medium (including paper, electronic, audio, and visual formats) that meets one or more of the following criteria:

   i. It is subject to a legal obligation requiring the university to responsibly manage the data.

   ii. It is substantive and relevant to the planning, managing, operating, documenting, staffing, or auditing of one or more major administrative functions, or multiple organizational units, of the university.

   iii. It is included in an official university report.

   iv. It is used to derive any data element that meets the above criteria.

SCOPE

This policy applies to:

- All individuals who handle Butler University data in any capacity, including:
  - Faculty, staff, and administrators
  - Students, student employees, and graduate assistants
  - Affiliates, visiting scholars, and research collaborators
  - Contractors, vendors, and service providers acting on behalf of the University
  - Any other person granted access to Butler University information systems or data

- All institutional data as defined by the policy.

EXCEPTIONS

Exceptions are not automatic and must be approved by the Chief Information Security Officer (in consultation with the General Counsel as necessary).

ADMINISTRATION

This policy shall be reviewed at a minimum, every three years, or when the following conditions occur:

- Security policy changes occur within IT
- University policy changes regarding the roles and responsibilities
- Federal guidelines regarding data change

RELATED POLICIES

- Acceptable Use Policy

REVISION HISTORY

- Revised by the CISO and Approved by University Cabinet on January 14, 2026
- Approved on April 7, 2020