Protection of University Data Policy

Date Established: 5/6/2010
Date Last Revised: 10/27/2025
Category: Information Technology
Responsible Office: Information Security Office
Responsible Executive: Vice President and Chief Information Officer

Summary

This policy establishes the framework for protecting sensitive and personally identifiable information, research findings, and proprietary data from unauthorized access, disclosure, alteration, or destruction.

Policy Statement

The University at Buffalo (UB, university) is committed to safeguarding the integrity and availability of all university data. UB employs robust technological measures, comprehensive data governance frameworks, and ongoing education and awareness programs to foster a culture of data security among the university community. Members of the university community must comply with all relevant laws, regulations, policies, and guidance governing data privacy and security.

Use of University Data

Access, collection, storage, or transmission of university data is a privilege granted to individuals based on their roles and responsibilities within a particular unit and must be approved by a data trustee prior to accessing data. Approval to use university data is contingent upon the unit's demonstrated operating needs, as well as the risk mitigation measures in place to protect the data. Data should only be used for legitimate academic, administrative, and research purposes, and any unauthorized access, use, or disclosure is strictly prohibited.

Storage of University Data

All university data must be classified and protected in accordance with the *Data Risk Classification Policy*. Use, processing, review, and storage of university data may occur only within environments which have been specified for use for the data classification in question. Category 1 Restricted Data and Category 2 Private Data cannot be accessed, collected, stored, or transmitted via non-secure environments. Examples of inappropriate environments/devices include but are not limited to:

- Cloud-based storage solutions which have not been approved through the UB software review and procurement process.
- Desk-top storage solutions which have not been approved through the UB software review and procurement process.
- Removable devices or hardware which are not owned by the university.
- Generative artificial intelligence (AI) applications which have not been approved through the UB software review and procurement process.

Implementing Technical Safeguards

UB utilizes encryption technologies to protect Category 1 Restricted Data and Category 2 Private Data during transmission and at rest; refer to the *Data Risk Classification Policy* to determine the data classification. Access controls, including role-based permissions and authentication mechanisms, restrict data access to authorized personnel only, minimizing the risk of data breaches. These technical controls include preventive, supporting, detection, and recovery controls.

UB Information Technology (UBIT) conducts security assessments and audits which are integral components of the technical safeguard framework, enabling continuous monitoring and evaluation of the effectiveness of security measures. UBIT encourages the use of secure data backup and recovery solutions to mitigate the impact of potential data loss incidents.

Reporting Exposure of University Data

All members of the university community, are obligated to report any suspected or confirmed exposure of university data or security breach of a system containing university data to the Information Security Office (ISO). All reports will be investigated in accordance with the university's Information Security Incident Response Plan. Instances of data exposure will be investigated, and remedial actions taken to address vulnerabilities and prevent recurrence. Exposed data will be handled with the utmost sensitivity and corrective measures will be implemented promptly to mitigate any potential impact on the integrity or availability of university data.

Compliance

Any individual who misuses university data is subject to disciplinary action in accordance with university policies, procedures, and applicable collective bargaining agreements. Any misuse of university data or IT resources may result in the limitation or revocation of access to university IT resources. Failure to comply with this policy may also constitute a breach of federal, state, or local laws.

Background

University policies and procedures must include controls to protect the integrity and availability of data and comply with laws and contractual obligations. Recognizing the critical role data plays in university operations, it is imperative that UBIT upholds the highest standards of data security by promoting a culture of responsible data stewardship across all departments and individuals.

Applicability

This policy applies to all university employees, students, and third-party vendors who access, manage, store, or in other capacities use university data. For data regulated by the Health Insurance Portability and Act (HIPAA), refer to the applicable UBIT HIPAA policies or contact the Director of UB HIPAA Compliance.

Definitions

Category 1 – Restricted Data

University data which is exempt from disclosure or release under the NYS Freedom of Information Law (FOIL). The NYS Information Security Breach and Notification Act requires the university to disclose any breach of the data to New York residents. (State entities must also notify non-residents; see the NYS Information Security Policy.)

Individuals who access, process, store, or in any other way handle Category 1 – Restricted Data must implement controls and security measures as required by relevant laws, regulations, and university policy. In instances where laws and/or regulations conflict with university policy, the more restrictive policy, law, or regulation governs.

Category 2 – Private Data

Includes university data not identified as Category 1 – Restricted Data, and data protected by state and federal regulations. This includes Family Educational Rights and Privacy Act (FERPA)-protected student records and electronic records that are specifically exempt from disclosure by the NYS FOIL.

Category 2 – Private Data must be protected to ensure that they are not disclosed in a FOIL request. Private data must be protected to ensure that they are only disclosed as required by law, including FOIL. Decisions about disclosure must be made by the Records Management Officer.

The National Institute Standards and Technology (NIST) Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations maps to the Category 2 – Private Data risk classification.

IT Resources

Any university asset used to process, access, manage or store electronic information.

Responsibility

Data Manager

University officials and their staff with operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data. Data Stewards may delegate data administration activities to Data Managers.

Data Owner

The University at Buffalo owns all university data, while individual units or departments may have stewardship responsibility for portions of such data.

- Administer activities delegated by data stewards.
- Maintain physical and system security and safeguards appropriate to the classification level of the data in their custody.

Data Steward

University official who has planning and policy-level responsibilities for data in their functional areas. Data Stewards are assigned by the Data Trustee.

- Adhere to the principles of least privilege and minimum-necessary.
- Create and maintain data documentation, including data dictionaries, data flow diagrams, and data lineage.
- Develop and maintain clear and consistent procedures for data access and use in keeping with university policies.
- Educate faculty, staff, and students on data-related matters.
- Ensure that training and awareness of the terms of this policy are provided.
- Ensure data in their functional area is accurate, consistent, and reliable.
- Oversee defined elements of institutional data.
- Implement and enforce data policies, standards, and practices, including definition of data ownership, access controls, data classification, and data lifecycle management.
- Maintain metadata – information about data elements, their definitions, and relationships.
- Manage data security in privacy, in conjunction with the ISO.
- Grant, renew, and revoke access to Data Managers and/or Data Users (as delegated by Data Trustees), as appropriate.
- Monitor compliance with this policy.
- Prevent unauthorized access to Category 1 Restricted Data and Category 2 Private Data.
- Report concerns and possible incidents to management for evaluation and response.
- Manage planning and policy-level matters for data in their functional areas.

Data Trustee

Senior leader of the university (i.e., vice president, vice provost, dean) who has responsibility for areas that have systems of record.

- Assign and oversee data stewards.
- Adhere to the principles of least privilege and minimum-necessary.
- Control university data by granting access, renewing access, and revoking access to Data Stewards, Data Managers, and/or Data Users. Data Trustees may delegate this responsibility to Data Stewards or Data Managers.
- Ensure that Data Stewards in their area are compliant with data governance principles.
- Establish data policies within their functional areas.
- Comply with legal and regulatory requirements specific to their domain.
- Promote data quality and use.
- Report concerns and possible incidents to management for evaluation and response.

Data User

An individual who uses university data as part of their assigned duties or to fulfill their role in the university community, with access as granted by a Data Trustee or Data Steward.

- Access, retrieve, update, process, analyze, store, distribute, or in other manners use university data for the legitimate and documented conduct of university business.
- Adhere to the principles of least privilege and minimum-necessary.
- Follow appropriate safeguards to protect data based on its classification.
- Follow all university policies, procedures, and standards related to data security classification and security level, including applicable federal and state laws.
- Implement appropriate safeguards to protect data.
- Maintain the confidentiality, integrity, and availability of university data.
- Report concerns and possible incidents to management for evaluation and response.
- Complete the Handling Data Safely training successfully, prior to receiving data access.
- Use data for the purposes in which access is granted.

Information Security Officer

- Conduct periodic security reviews of systems approved for storing and handling protected data.
- Develop and deliver enterprise information security strategy, governance, and policy in support of institutional goals. Information Security incidents must be reported to the ISO.
- Review and approve departmental collection, storage, and transmission of data when necessary, according to its classification.
- Serve on the Cloud Services Review Committee.

Vice President and Chief Information Officer (VPCIO)

- Provide leadership for development and delivery of information technology (IT) services to the university.

- Oversee an enterprise IT services organization, Computing, and Information Technology (CIT), and work in partnership with UB's schools, colleges, and administrative IT units to enable a unified and productive IT experience for students, faculty, and staff.

Contact Information

Contact	Phone	Email
Office of the Vice President and Chief Information Officer	716-645-7979	cio@buffalo.edu
Information Security Office	716-645-6997	sec-office@buffalo.edu
Director of UB HIPAA Compliance	716-829-3172	hipaa-compliance@buffalo.edu

Related Information

University Links

- Data Access Procedure
- Data Risk Classification Policy
- Information Security Incident Response Plan
- Records Management
- Social Security Number Policy
- Standards for Protecting University Data
- UB Information Technology
- UB Information Technology - Information Security Office
- UB Information Technology – HIPAA Policy
- UB Information Technology – Minimum Security Standards for Desktops, Laptops, Mobile, and Other Endpoint Devices
- UB Information Technology – Minimum Server Security and Hardening Standards
- UBIT HIPAA Policy

Related Links

- Gramm-Leach-Bliley Act
- Health information Privacy
- New York State Cyber Incident Response Standard
- New York State Enterprise Information Security Office
- New York State Information Security Policy
- New York State Office of Information Technology Services - Breach Notification
- Payment Card Industry Data Security Standards Council
- Privacy Act of 1974 (includes protection of Social Security Numbers)

History

October 2025	Full review. Update the policy to:
	• Revise and expand the following sections:
	  ○ Summary
	  ○ Policy Statement
	  ○ Use of University Data
	  ○ Reporting Exposure of University Data (previously Reporting Potential of Actual Exposure of University Data)
	  ○ Compliance
	  ○ Background
	• Add the following sections
	  ○ Storage of University Data
	  ○ Implementing Technical Safeguards
	• Add a definition for IT Resources
	• Add responsibilities for:
	  ○ Data Manager
	  ○ Data Owner
	  ○ Data Steward
	• Expand the responsibilities for the:
	  ○ Data Trustee
	  ○ Data User
	  ○ Information Security Officer
	  ○ Vice President and Chief Information Officer
	• Removed Contact Information for Records Management Office
	• Removed the following outdated links
	  ○ UB HIPAA Webpage
	  ○ Vendor Questionnaire for Information Technology Purchases

April 2018	Full review. Updated the policy to: • Change the title from *Protection of Regulated Private Data Policy* to *Protection of University Data Policy* • Update content to reflect the revised *Data Risk Classification Policy* • Update references in the Related Information section • Remove procedural language • Update data role terminology • Add HIPAA compliance reference • Direct readers to the *Data Risk Classification Policy* for data categories