Data Risk Classification Policy

Date Established: 5/24/2010
Date Last Revised: 11/22/2024
Category: Information Technology
Responsible Office: Vice President and Chief Information Officer
Responsible Executive: Vice President and Chief Information Officer

Summary

UB classifies data into three risk-based categories to regulate access to, use of, and necessary precautions required to the protect university data. This policy provides a classification framework based on relevant legal and regulatory requirements to which the university is subject and provides a framework for classifying university data based in its level of sensitivity, value, and criticality to determine baseline security controls and protect data.

Policy Statement

The University at Buffalo (UB, university) is committed to protecting the confidentiality, integrity, and availability of university data. All university data must be classified into one of three data classification categories:

Category 1 – Restricted Data

Protection of Category 1 – Restricted Data is required by law or regulation. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Restricted data includes the definition of private information in the New York State (NYS) *Security Breach and Notification Act* as a foundation: bank account, credit card, debit card numbers; social security numbers; state-issued driver license numbers; and state-issued non-driver identification numbers. To this list, university policy adds protected health information (PHI), computer passwords, other computer access protection data, passport numbers, as well as research data which requires the use of PHI and personally identifiable information (PII).

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, university policies, and supporting standards. In instances where laws and/or regulations conflict with university policy, the more restrictive policy, law, or regulation governs.

Category 2 – Private Data

Category 2 – Private Data includes university data which is not identified as Category 1 – Restricted Data, but which is 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 New York State (NYS) Freedom of Information Law (FOIL), as well as Research Foundation (RF) proprietary data, and all University at Buffalo research data.

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

Category 3 – Public Data

Category 3 – Public Data includes all other university data which is not included in Category 1 – Restricted Data or Category 2 – Private Data. Category 3 – Public data includes any data that is releasable in accordance with FOIL. This category also includes general access data, such as that available on unauthenticated portions of UB's website. Public data has no requirements for confidentiality; however, systems housing the data should take reasonable measures to protect its accuracy.

Compliance

UB complies with applicable regulatory requirements concerning data breaches including but not limited to the NYS Information Security Breach and Notification Act, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA), FERPA, and Payment Card Industry (PCI). In instances of uncertainty regarding data classification the most restrictive data classification must be applied.

Violations of this policy and all related policies, standards, or guidance documents may result in financial or reputational losses and/or legal actions for the university, as well as any individuals responsible for handling and protecting university data.

Data Users who misuse data and/or illegally access data are subject to sanctions or penalties in accordance with employee relations policies. Sanctions or penalties are based on the standards outlined in university policy, state or federal regulations, and the appropriate collective bargaining agreements. Individuals found to be in violation of this policy and other university policies related restricted data may face corrective action commensurate with the violation, up to and including termination or expulsion.

Individuals who suspect a misuse of standards and policies related to Category 1 or Category 2 data must report their concerns to their applicable Data Trustee or the Information Security Officer (ISO).

Background

University academic and administrative data are valuable assets and often contain detailed information about the university, as well as personal information about faculty, staff, students, and other third parties affiliated with the university. Protecting this information is essential.

Applicability

This policy applies to all data or information created, collected, stored, or processed by the university, whether in electronic or non-electronic formats. Data that is personal to the operator of a system and stored on a university information technology (IT) resource as a result of incidental personal use is not considered university data.

Definitions:

Data Administration: The responsibility for the activities of data administration, including detailed data definition, is shared among the Data Stewards, Data Managers, and the Vice President and Chief Information Officer (VPCIO).

Senior Leader: Designated as the president, provost, vice provosts, executive vice presidents, vice presidents, associate vice presidents, and deans who are eligible for access to enterprise-wide aggregate and summary university data. Senior management is authorized to delegate access of enterprise-wide aggregate and summary university data, as deemed appropriate.

Third Party: Any entity which is legally separate from the University at Buffalo, but who the university may partner with when conducting business.

University Data: Items of information which are collected, maintained, and utilized by the university for the purpose of carrying out institutional business. Includes centrally stored data, as well as data generated and stored in university departments and decanal units All university data is required to have an identified Data Trustee.

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 needs and 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.
- Successfully complete the Handling Data Safely training, prior to receiving data access.

- Use data for the purposes in which access is granted.

Information Security Officer (ISO)

- 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.

Information Security and Privacy Advisory Committee (ISPAC):

- Evaluate, develop, and recommend information security and privacy policies, procedures, and operations vital to protecting and sustaining the university's mission.

Records Management Officer

- Determine appropriate record disclosures pertaining to FOIL requests.

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	vpcio@buffalo.edu
Information Security Office	716-645-6997	sec-office@buffalo.edu
Records Management Officer	716-645-1786	-

Related Information

University Links

- Data Access Procedure
- Data Risk Classification Policy
- Data Governance

- Deleting Data Securely from Devices
- Desktop/Laptop Security by Disk Encryption
- Freedom of Information Law (FOIL)
- Handling Data Safely Training
- Mobile Communication Devices
- Protection of University Data Policy
- Records Management
- Record Retention and Disposition Policy
- Safety and Security Camera Applicable Use Policy
- Social Security Number (SSN) Access Request Procedure
- Social Security Number (SSN) Usage Guidelines
- Standards for Protecting Category 2 - Private Data
- Storing Restricted Data in UBbox
- Technology Guidance for Remote Computing and Telecommuting
- Tips for Protecting UB Data When Working with Vendors or Others
- UB Information Technology
- UB Information Technology – Keeping You and Your Devices Safe at UB
- UB Minimum Security Standards for Desktops, Laptops, Mobile and Other Endpoint Devices
- UB Minimum Server Security and Hardening Standards
- UBIT HIPAA Policy
- UBIT Policy, HIPAA, FERPA and the Breach Notification Act
- What is Restricted Data?

Related Links

- Family and Educational Rights and Privacy Act (FERPA)
- FIPS 140-2 – Security Requirements for Cryptographic Modules
- Gramm-Leach-Bliley Act
- Health Information Privacy - Summary of the HIPAA Privacy Rule
- National Institute of Standards and Technology (NIST) 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- National Institute of Standards and Technology (NIST) - Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)
- New York State Freedom of Information Law
- New York State Office of Information Technology Services Breach and Notification Act
- New York State Office of Information Technology Services Information Classification Standard
- New York State Office of Information Technology Services Information Security Policy
- Privacy Act of 1974
- Protected Health Information (HIPAA regulated)
- State University of New York Privacy Policy

History

Policy Revision History

November 2024

Full review. Updated the policy to:

- Remove the data classification examples (chart format)
- Revise the Compliance, Background, and Applicability sections
- Include position definitions in the Responsibility section
- Add definitions for Data Administration, Senior Leader, Third Party, and University Data
- Update responsibilities for the Data Manager, Data Steward, Data Trustee, Data User, and VPCIO
- Add responsibilities for the Data Owner, ISO, and ISPAC

October 2023

Updated the data classification chart examples to include demographic data as Category 2 - Private Data

February 2022

- Updated the data classification chart to:
  - Remove references to the Minimum-Security Standard, per National Institute of Standards and Technology 800-53 (Data Risk Classification Category column)
  - Add the statement: "Institutional risk definitions and thresholds are congruent with Federal Information Processing Standards (FIPS) 199 *Categorization of Information and Information Systems"*
- Retire the *Data Risk Classification Appendix* including the Security Standard Crosswalks

September 2021

Updated the data classification chart examples to move donor contact information from Category 1 - Restricted Data to Category 2 - Private Data

April 2018

Full review. Updated the policy to:

- Change the title of the policy from *Data Classification Standard/Data Use Standard* to *Data Risk Classification*
- Change the number of classification categories from four (i.e., Category I: Regulated Private Data; Category II: Protected Data; Category III: Internal Use Data; Category IV: Public Data) to three (i.e., Category 1 – Restricted Data, Category 2 – Private Data, Category 3 – Public Data)
  - This change aligns the UB categories with the New York State Office of Information Technology Services *Information Classification Standard*
- Revise data role terminology
- Add HIPAA compliance reference

- Provide additional data risk classification guidance including
  - FIPS 199 Security Categorization Definitions
  - Security Standard Crosswalks
  - Data Risk Classification Examples