Protection of University Data Policy

**Category:** Information Technology  
**Responsible Office:** Information Security Office  
**Date Established:** 01/09/2009  
**Responsible Executive:** Vice President and Chief Information Officer  
**Date Last Updated:** 11/28/2017

**Summary**

UB data must be protected to safeguard privacy, reduce the threat of identity theft, and maintain compliance with state and federal laws and regulations.

**Policy Statement**

The University at Buffalo (UB, university) is committed to collecting, handling, storing, and using university data properly and securely. This policy establishes a framework of safeguards to:

- Protect university data from accidental or intentional alteration or theft or other risks
- Comply with applicable laws and contractual requirements
- Increase awareness of the need to protect university data

**Use of University Data**

Access, collection, storage, and/or transmission of university data must be approved by a data trustee in accordance with the *Data Access Procedure*. 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. Risk mitigation measures include, but are not limited to the collection, storage, and transmission of these data by third-party service providers (e.g., cloud services).

**Reporting Potential or Actual Exposure of University Data**

A suspected or confirmed exposure of university data, or security breach of a system containing university data, must be immediately reported to the Information Security Officer (ISO).

**Compliance**

An employee or student who breaches the confidentiality of Category 1- Restricted Data or Category 2- Private Data, may be subject to disciplinary action in accordance with university policy and procedures.

**Background**

University information is a valuable asset that requires appropriate protection. University policies and procedures must include controls to protect the confidentiality, integrity, and availability of data and comply with laws and contractual obligations.
In order to comply with state and federal laws and regulations, university policies and procedures must include proper controls to protect the confidentiality, integrity, and availability of data classifications that are restricted and/or protected.

**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 HIPAA policies.

**Definitions**

**Category 1 - Restricted**

Protection of the data is required by law/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 Security and Breach 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, and passport numbers.

Category 1 - Restricted data are exempt from disclosure/release under the *New York State Freedom of Information Law* (FOIL). The *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 *New York State Information Security Policy*.)

Individuals who access, process, store, or in any other way handle Category 1 Restricted data are required to implement controls and security measures as required by relevant laws and/or regulations in addition to any university policy. In instances where laws and/or regulations conflict with university policy, the more restrictive policy, law, or regulation should be enacted.

**Category 2 - Private**

Includes university data not identified as Category 1 - Restricted data, but includes 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 exempted from disclosure by the New York State FOIL.

Private data must be protected to ensure that they are not disclosed in a FOIL request. FOIL excludes data that if disclosed would constitute an unwarranted invasion of personal privacy.

The *NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* maps to the Category 2 - Private data risk classification.
Data Trustees
Senior leaders of the university (i.e., vice presidents, vice provosts and deans) who have responsibility for areas that have systems of record.

Data Users
Individuals who need and use university data as part of their assigned duties or in fulfillment of their role in the university community.

Responsibility

Data Trustee
- Ensure that data stewards in their area are compliant with data governance principles.

Data User
- Follow appropriate safeguards to protect data based on its classification

Information Security Officer
- Review and approve departmental collection, storage, and transmission of data when necessary according to its classification.
- Serve on the Cloud Services Review Committee.
- Conduct periodic security reviews of systems approved for storing and handling protected data.

Vendors
- Complete the Vendor Questionnaire (obtained from Purchasing).

Vice President and Chief Information Officer
- Responsible for the leadership and oversight of all components of UB’s Information Technology.

Contact Information

Office of the Vice President and Chief Information Officer
517 Capen Hall
Buffalo, NY 14260
Phone: 716-645-7979
Email: cio@buffalo.edu
Website: http://wwwbuffalo.edu/ubit.html

Information Security Office
201 Computing Center
Buffalo, NY 14260
Phone: 716-645-6997
Related Information

University Links:
Data Risk Classification Policy
Data Access Procedure
Securing Network-Connected Devices Policy
Social Security Number Policy

Forms:
Vendor Questionnaire (Vendors obtain this form directly from Purchasing)

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 Enterprise Information Security Office Breach Notification
New York State Information Security Policy
Payment Card Industry Data Security Standards Council
Privacy Act of 1974 (includes protection of Social Security Numbers)

History
November 2017 Full review. Updated policy to:
- Revise the title from Protection of Regulated Private Data Policy to Protection of University Data Policy
- Update content to reflect revised Data Risk Classification Policy
- Update references to Related Information section
- Remove procedural language
- Update data role terminology
- Add HIPAA compliance reference
- Update data role terminology
- Direct readers to Data Risk Classification Policy for data categories, rather than describe them in the policy
Guidance Document: Data Access Procedure

Category: Information Technology, Information Security  
Date Established: 07/06/2013
Responsible Office: Vice President and Chief Information Officer  
Date Last Updated: 10/30/2017
Responsible Executive: Vice President and Chief Information Officer

Summary

The Data Access Procedure:

- Classifies university data into functional areas
- Assigns the data trustees for each area
- Defines the roles, responsibilities, data management environment, and procedure for granting access to UB’s non-public data
- Applies to university data in hard copy and electronic format.
- Supplements the Protection of University Data Policy and the Data Classification Risk Policy

Individuals who access, retrieve, update, process, analyze, store, distribute, or in other manners use university data are responsible for securing and protecting the data in accordance with the Protection of University Data Policy and Data Risk Classification Policy.

The University at Buffalo is the data owner of all university data. Individual units or departments have stewardship responsibilities for portions of the data. Individuals are assigned data roles to access, retrieve, update, process, analyze, store, distribute, or in other manners use university data in order to carry out institutional business in keeping with the Data Risk Classification Policy.

All university data must be classified and protected in accordance with the Data Risk Classification Policy:

- Non-public data is classified as Category 1 - Restricted Data and Category 2 - Private Data.
- Non-public data must be protected throughout its life cycle in a manner consistent with its classification.
- Public data is classified as Category 3 data. Public data has no requirements for confidentiality, however, systems housing the data should take reasonable measures to protect its accuracy.

Commented [CK1]: FYI - this document needs Jeff and Brice's approval
The Data Access Procedure does not apply to research data, scholarly work of faculty and students, and intellectual property.

A separate data access procedure is in place for HIPAA regulated data. Contact the Director of HIPAA Compliance (hipaa-compliance@buffalo.edu) for more information.

Definitions, Roles, and Responsibilities

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition, Roles, and Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Administration</td>
<td>The responsibility for the activities of data administration, including detailed data definition, is shared among the Data Stewards, Data Managers, and the VPCIO.</td>
</tr>
<tr>
<td>Data Manager</td>
<td>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.</td>
</tr>
<tr>
<td>Data Owner</td>
<td>The University at Buffalo is the data owner of all university data; individual units or departments have stewardship responsibilities for portions of the data.</td>
</tr>
</tbody>
</table>
| Data Steward       | • Assigned by Data Trustees  
                      • Responsible for planning and policy-level responsibilities for data in their functional areas  
                      • Have supervisory responsibilities for defined elements of institutional data  
                      • May grant, renew, and revoke access to Data Managers and/or Data Users (as delegated by Data Trustees)  
                      • Develop and maintain clear and consistent procedures for data access and use in keeping with university policies  
                      • Prevent unauthorized access to Category 1 Restricted Data and Category 2 Private Data  
                      • Ensure that training and awareness of the terms of this procedure are provided  
                      • Monitor compliance with this procedure                                                                                                                                  |
| Data Trustee       | • Senior leaders of the university (vice-presidents, vice-provosts, and deans) who have responsibility for areas that have systems of record                                                                                                         |
### Data Access Procedure

- Responsible for ensuring that data stewards, data managers, and data users in their respective area(s) are compliant with data governance principles
- Classify university data in accordance with the *Data Risk Classification Policy*
- 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
- Assign Data Stewards who function as described above
- Data Trustees may work directly with Data Stewards, Data Managers, and/or Data Users

**Data Users**

- Individual with data access as granted by a Data Trustee or Data Steward
- Complete and sign *University Administrative Information Systems: Access to Information Compliance Form* outlining responsibilities, prior to receiving data access
- Access, retrieve, update, process, analyze, store, distribute, or in other manners use university data for the legitimate and documented conduct of university business
- Use data for the purposes in which access is granted. Sanctions or penalties for misuse or illegal use of data access will be imposed on Data Users 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.
- Comply with the *Data Risk Classification Policy* and secure Category 1 Restricted Data and Category 2 Private Data.

**Functional Areas of University Data**

<table>
<thead>
<tr>
<th>The functional areas of university data are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admissions (Undergraduate data only)</td>
</tr>
<tr>
<td>AP Credit</td>
</tr>
<tr>
<td>Athletics</td>
</tr>
<tr>
<td>ePay</td>
</tr>
<tr>
<td>Financial Aid</td>
</tr>
<tr>
<td><strong>Graduate Admissions</strong></td>
</tr>
<tr>
<td>Graduate School (GRE and TOEFL)</td>
</tr>
</tbody>
</table>

---

**Comments**

- **Commented [SK4]:** By whom? Should that be defined here?
- **Commented [LP5]:** Sentences written in the passive voice usually don’t specify who is performing the action. We recommend writing in the active voice to address this concern.
- **Commented [CK6]:** Pam—how is this? Or should I be more specific?
- **NOTE FROM JEFF:** Not sure. It would minimally start with the supervisor, but probably also involve Employee Relations. Does HR have a written sanction policy we can refer to?
- **Commented [LP7R6]:** We can check with Chris Putrino (Director of Employee Relations) about any sanction policies.
- **Commented [SK8]:** Why is this being limited to InfoSource data? There’s a great deal of data at the institution that is not in InfoSource. Could/should it also benefit from this?
- **Commented [CK9]:** Could ISPAC compile a list? Is there a penultimate list?
- **Commented [CK10]:** Jeff revised
- **Commented [CK11]:** Information from [https://www.buffalo.edu/content/wip/ubinfosource/authenticated-pw/getting-started/requesting-data-access.html](https://www.buffalo.edu/content/wip/ubinfosource/authenticated-pw/getting-started/requesting-data-access.html)
- **Commented [CK12]:** per Policy Review Group 11/2017
### Information Security and Privacy Advisory Committee (ISPAC)

ISPAC is responsible for evaluating, developing, and recommending information security and privacy policies, procedures, and operations vital to protecting and sustaining the university's mission.

### Information Security Officer (ISO)

Responsible for development and delivery of enterprise information security strategy, governance and policy in support of institutional goals. Information security incidents must be reported to the ISO.

### InfoSource

UB InfoSource is a data delivery mechanism based on an Oracle database. It consists of a collection of information from multiple production databases. It is physically separated from application data and doesn't impact on-line operations. The information is read only and cannot be changed.

UB InfoSource is not intended as a replacement for any other systems. It incorporates data contained in a variety of disparate administrative systems into a single source that allows the client to choose the cycle, population, and format of the output generated.

### Non-Public Data

According to the *Data Classification Risk Policy*, Category 1 - Restricted Data and Category 2 - Private Data are considered non-public data.

### Senior Management

- Designated as the president, provost, vice provosts, executive vice presidents, vice presidents, associate vice presidents, and deans
- Eligible for access to enterprise-wide aggregate and summary university data.
**Data Access Procedure**

- Authorized to delegate access of enterprise-wide aggregate and summary university data, as deemed appropriate.

**Shadow system, extension system, extender system**

**University Data**

Defined as items of information that 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.

**Vice President and Chief Information Officer (VPCIO)**

The VPCIO provides leadership for development and delivery of information technology (IT) services to the university. The VPCIO oversees an enterprise IT services organization, Computing and Information Technology (CIT), and works in partnership with UB’s schools, colleges and administrative IT units to enable a unified and productive IT experience for students, faculty and staff.

<table>
<thead>
<tr>
<th>Functional Areas and their Respective Data Trustees</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Functional Area</strong></td>
</tr>
<tr>
<td>Admissions (Undergraduate data only)</td>
</tr>
<tr>
<td>AP Credit</td>
</tr>
<tr>
<td>Asset Management (Inventory)</td>
</tr>
<tr>
<td>Athletics</td>
</tr>
<tr>
<td>Donor Contact Information and non-public gift information</td>
</tr>
</tbody>
</table>

Commented [CK14]: Stop here

Commented [CK15]: Information from https://www.buffalo.edu/content/www/ubinfosource/authenticated-pw/getting-started/requesting-data-access.html

Commented [CK16]: Chris Clune: Recommended striking individual names
### Guidelines

Data Users who access, retrieve, update, process, analyze, store, distribute or in other manners use university data for the legitimate and documented conduct of university business must agree to the
guidelines below. As applicable, Data Trustees and/or Data Stewards issue detailed guidelines for each functional area.

1. Data Trustees and their delegates grant and revoke access to Category 1- Restricted Data and Category 2- Private Data (non-public) university data. Access is granted only to those with a legitimate business need for the data.
2. Data access is renewed on an annual basis, or more often as needed.
3. Data access is granted only for legitimate purposes and within the terms articulated in applicable university policies.
4. Data access rights are non-transferable.
5. Data Users are explicitly prohibited from releasing, sharing, or transmitting data to others, other than for the legitimate business purposes for which the data access was granted.
6. Data Users are explicitly prohibited from using data for purposes other than those for which the data access was granted.
7. Data Users and their supervisors must complete the form, Access to University Information, before they will be given access to Category 1- Restricted Data and Category 2 - Private Data (non-public) university data. Completion of this form ensures that Data Users will abide by the requirements set forth in the Data Risk Classification Policy.
8. Access to Social Security Numbers (SSN) in UB InfoSource is highly restricted and granted only to employees with a specific legal or business need that cannot be met in another way.
9. In order to request access to SSNs in UB InfoSource, individuals are required to complete the Social Security Number Data Access Request, stating the legal statute and/or business need for SSNs. A committee composed of several Data Trustees and the ISO reviews all SSN access requests.

10. Extracts of data, data feeds, and data within shadow systems, extension systems, extender systems, or other applicable systems that store university data have the same classification level and utilize the same protective measures as the same data in the systems of record.
11. Any shadow system, extension system, extender system, or other applicable system that university data must be disclosed to the appropriate data trustee and the ISO is required.
12. Computer systems and devices used to support data must adhere to the specific, protective measures as set forth in the Server Security and Hardening Standards and the Security Standards for Desktops, Laptops, Mobile, and Other Endpoint Devices.

Compliance

Violations of this procedure will result in appropriate disciplinary measures in accordance with university policies, applicable collective bargaining agreements, and state and federal laws. For HIPAA-regulated data, please refer to applicable HIPAA policies.

Contact Information

Vice President and Chief Information Officer
Related Documents

University Documents:

- Access to University Information (form)
- Data Risk Classification Policy
- Social Security Number Data Access Request (form)
- Social Security Number Usage Policy
- Social Security Number usage Procedure
- UBIT HIPAA Protected Health Information Security Sanction Policy
- UBIT HIPPA Protected Health Information Security Policy
- University Administrative Information Systems: Access to Information Compliance (Form)
- User Agreement (form)

OTHER DOCUMENTS:

- New York State Information Security Policy
<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>CIO</td>
<td>07/16/2013</td>
<td>Published version on university policy website “Information Security: Data Access and Security Policy”</td>
</tr>
</tbody>
</table>
| 2.0     | Murphy, Jeff | Summer 2017, various dates. | Replace policy with guidance document (procedures).  
Revised document name, "Data Access Procedures."  
Separate procedural information from policy.  
Reconcile data roles/data terminology |
| 2.1     | Murphy, Jeff | 10/02/2017    | Updated functional areas of university data, per InfoSource.             |
| 3.0     | Murphy, Jeff | 10/26/2017    | Revisions suggested from Kara Saunders, Chris Clune, and Pam Lojacono.   |
| 4.0     | Murphy, Jeff | 10/30/2017    | Revisions from Pam Lojacono incorporated into draft.                    |
| 4.1     | Murphy, Jeff | 11/28/2017    | Revisions from Policy Review group incorporated into draft.             |