



Updated Policy: Data Access, Security, and Acceptable Use

Policy Statement

The University requires all users of University administrative data¹ to utilize the data in a manner consistent with the University's requirements for security and confidentiality, as well as with state and federal legal protections and laws².

Access to University administrative data is granted by data custodians and trustees who are required to develop and maintain clear and consistent procedures for access and use of the data, prevent unauthorized access, and protect restricted, non-public data. Data custodians and trustees³ also classify University data by level of sensitivity and risk, taking into account federal and state legal protections, contractual agreements, ethical considerations, and strategic worth to the institution.

Employees will be asked to complete and sign an "Access to University Information" form before being granted access to University administrative data.

Access to and use of University administrative data is non-transferrable. Administrative data users may not transfer their data access rights to others, release administrative data to others, or use data for purposes other than those for which access was granted. Each individual user of administrative data must apply to the appropriate data custodian or trustee to obtain access.

Supervisors of student employees with access to University administrative data are responsible for oversight to ensure that students are informed of their responsibilities and that students access and utilize this data in a manner that is consistent with the university's need for security and confidentiality and compliance with state and federal legal protections and laws.

This policy applies to the access and acceptable use of University administrative data by University employees. Data access and acceptable use by third party vendors is discussed in a separate policy under development.

Reason for Policy

Information plays a vital role in the University's educational, research, operational, and public service activities. The University facilitates access to data by those with official educational and administrative responsibilities within the institution, recognizes the importance of taking necessary steps to protect information/data, ensures that data access restrictions are based on legal, ethical, and practical considerations, and informs trustees, custodians, and users of University administrative data of their legal and ethical responsibilities.

The purpose of this policy is to ensure the protection of the University's information resources from accidental or intentional unauthorized access or damage, while preserving the open, information-sharing requirements of the academic culture.

¹ University administrative data includes centrally-stored data as well as data locally-generated and stored in decanal areas, departments and other distributed University units.

² Specific legislation governs access to student educational records (FERPA), customer financial information records (GLBA), and protected, individually-identified health information records (HIPAA).

³ See page 4 for contact information for data trustees and their areas.

Entities Affected by This Policy

All members of the University at Buffalo community

Any University employee granted access to University at Buffalo administrative data

Who Should Read This Policy

All members of the University at Buffalo community

Any University employee granted access to University at Buffalo administrative data

Website Address for Policies: <http://www.itpolicies.buffalo.edu/>

Related Documents

| Federal & State Laws and Regulations | Scope: What Entities Do Laws & Regulations Apply To? |
|--|--|
| NYS Internet Security & Privacy Act | <ul style="list-style-type: none"> » Requires a Privacy policy statement on campus web sites » Limits disclosure of personal information collected on campus web sites |
| Federal Privacy Act of 1974 | <ul style="list-style-type: none"> » Federal, state, or local government agencies requesting individuals to disclose social security numbers must state whether disclosure is mandatory or voluntary. If mandatory, the statutory or other authority for collection must be cited and how the SSN will be used must be stated. |
| NY State Law: Limitations on the Use of Social Security Numbers | <ul style="list-style-type: none"> » Tracks the Federal Privacy Act of 1974, limiting the collection and use of social security numbers by colleges/universities » Where there is no legal basis for a request to disclose SSNs, an individual may refuse to disclose the SSN |
| Electronic Communications Privacy Act | <ul style="list-style-type: none"> » Broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral, or electronic communication. » Also prohibits unauthorized access to or disclosure of electronically-stored wired and electronic communications |
| Family Educational Rights and Privacy Act (FERPA) FERPA Privacy Resources | <ul style="list-style-type: none"> » Covers student educational records, including grades, degrees, transcripts, and enrollment status » Applies to all university personnel who manage, maintain, use, or handle student educational records, and their supervisors » Requires schools to minimize collection and use of students' social security numbers: SSNs should be collected only for the purpose of processing student loans, employment, and to meet other legal obligations |
| Gramm-Leach-Bliley Act (GLBA) GLBA Resources | <ul style="list-style-type: none"> » Covers customer financial and personal information records, including account balances and loan information <p>Covered Units</p> <ul style="list-style-type: none"> » Student Financial Services/Office of the Provost » Financial Services Offices in the Decanal Areas (e.g., School of Medicine) |
| Health Insurance Portability and Accountability Act of 1996 (HIPAA) HIPAA Resources Impact of HIPAA's Privacy Rule | <p>Covered Units: UB HIPAA Web Site</p> <ul style="list-style-type: none"> » University Health care providers » Employee-sponsored health plans (RF) » Research protocols using individually-identifiable health information |
| USA PATRIOT Act: PATRIOT Act Resources | <p>Amends FERPA, ECPA, and Foreign Intelligence Surveillance Act (FISA) to permit release of personally identifiable information from student educational records without the consent of the student or parent</p> <ul style="list-style-type: none"> » to the Attorney General of the U.S. or his designee in response to an ex parte order in connection with the investigation or prosecution of terrorist crimes » to comply with a lawfully issued subpoena or court order » in the case of an immediate threat to the health or safety of students or other individuals » to the INS if the student has signed a Form I-20 » to the INS for any student attending on an M-1 or J-1 visa |
| SEVIS Student & Exchange Visitor Information System | Covers international student records: admissions, academic, and disciplinary information (established in USA PATRIOT Act) |

| |
|--|
| University Documents |
| UB IT Policies Web Site: http://www.itpolicies.buffalo.edu |
| Computer & Network Use (CIT) |
| Conditions of Use (CIT) |
| Cyber Security Policy |
| Social Security Number Policy |
| MyPhoto Classlists Pilot: Faculty Information and Use Guidelines– Under Review |

Contacts

Direct specific questions about this policy and the classification of data to the following offices and data trustees. See the MyUB Infosource link for information about acquiring access to Infosource data. See the appropriate Dean or Department head for information about acquiring access to non-central administrative data.

| Type of Administrative Data | Subject | Contact | Telephone |
|--|------------------------------|---|--------------------|
| | Policy Clarification | Chief Information Officer | 645-7979 |
| <i>Central University Administrative Data</i> | Admissions Data | Associate Director of Admissions | 645-7785 |
| | Athletics Data | Senior Associate Athletic Director | 645-3454 |
| | CASA | Assistant Vice Provost, OIA | 645-2791 |
| | E-mail Addresses | Director, Technical Services | 645-3582 |
| | Employee Data State or RF | Manager, Information Resources Personnel Services | 645-5000 ext. 1279 |
| | Financial Data | Director, Budget Services | 645-5000 ext. 1351 |
| | Graduate School Data | Assistant Dean, Graduate School | 645-2939 |
| | Information Technology Data | Vice President and CIO | 645-7979 |
| | Inventory | Director, Inventory Services | 645-5000 ext. 1110 |
| | Student Academic Data | Sr. Assoc Vice Provost and Director of Student Academic Records and Financial Services | 645-2450 |
| UBF Data: Financial | Exec. Director, UBF | 645-3011 | |
| <i>Non-Central Administrative Data⁴</i> | Alumni Data | Vice President for University Advancement See the <i>Alumni Data Privacy Policy</i> : http://www.alumni.buffalo.edu/privacy.html | 645-2925, ext. 150 |
| | HIPAA Compliance | UB HIPAA Compliance Officer | 829-3172 |
| | Other | Appropriate Dean or Department Head | |

⁴ Non-central University administrative data is data generated and stored in schools and departments (in the distributed units)

Definitions

The following definitions apply to terms used in this policy.

| Term | Definition |
|--|---|
| Data Custodian (Owner) | <p>An individual who has responsibility for managing University information resources. All University data must have an identified Data Custodian. Data Custodians support the mission of the University and facilitate the conduct of University business by ensuring that access to data is granted as needed for legitimate purposes and within the terms articulated in these and other University policies.</p> <p>Data Custodians include the Provost, Vice Provost and Dean of Undergraduate Education, Executive Vice President for Finance and Operations, Vice President and Chief Information Officer, Vice President for External Affairs, Vice President for Research, and the Vice President for Student Affairs.</p> |
| Data Trustee (Access Administrator) | <p>Each Data Custodian may designate one or more Data Trustees to execute day-to-day custodial responsibilities. In practice, Data Trustees are those persons primarily responsible for the accuracy, integrity, and privacy of University data. The Data Trustee for non-central administrative data is the appropriate Dean or Department Head.</p> |
| Administrative Data User | <p>An administrative data user is any person who has been granted authorization by a Data Custodian or Data Trustee to retrieve, update, process, analyze, or distribute data in the conduct of University business. Administrative data users are responsible for their use of the data to which they are granted access. Sanctions or penalties for misuse or illegal use of data access will be imposed on administrative data users based on the standards outline in University policy, state or federal regulations, and the appropriate collective bargaining agreements. Administrative data users must complete and sign an online “user agreement” outlining their responsibilities, before receiving access to data.</p> |
| Functional Areas of University Administrative Data | <p>The eleven functional administrative areas of University InfoSource data are Admissions, Athletics, CASA, E-Mail Addresses, Employee, Financial, Graduate School, Information Technology, Inventory, Student Services, UBF Financial.</p> |
| University Administrative Data | <p>University Administrative data include centrally-stored InfoSource data as well as administrative data generated and stored in University decanal areas and departments. The policy applies to Administrative data, in any form: hard copy/printed reports and any form of online (electronic) data.</p> |

Responsibilities

| Area | Responsibility |
|---|--|
| Vice President and CIO | <p>Manages access to University data in accordance with established policies and procedures:</p> <ul style="list-style-type: none"> ▪ Administers the information resource but in no sense dictates the use of University data nor determines individual access rights ▪ May delegate specific responsibilities to members of his/her staff ▪ Assists in the mediation and resolution of disputes regarding data policies and procedures |
| Director of Administrative Computing Services | <p>Implements, monitors, and coordinates standards, procedures, and guidelines necessary to administer access to University administrative data:</p> <ul style="list-style-type: none"> ▪ Suggests security considerations and guidelines to be used by Data Custodians and Data Trustees in granting access to administrative data users ▪ Establishes procedures to confirm the identities of Data Custodians and Data Trustees granting access to administrative data users ▪ Disseminates guidelines to be followed by administrative data users ▪ Implements password and other procedures and technology to restrict access to the University's administrative data ▪ Provides Data Custodians and Data Trustees access to reports, enabling them to verify that access has been granted only to authorized users and that the level of access granted is appropriate |
| Data Custodians | <ul style="list-style-type: none"> ▪ Manage University information resources. ▪ Ensure that access to data is granted as needed for legitimate purposes and within the terms articulated in this policy ▪ Ensure that training and awareness of the terms of this policy are provided ▪ Monitor compliance with policy |
| Data Trustees | <ul style="list-style-type: none"> ▪ Evaluate and respond to requests for access to data for which responsibility is assigned ▪ Determine the degree of access to data for which responsibility is assigned ▪ Ensure that access procedures include <ul style="list-style-type: none"> ○ Maintenance of an audit trail, i.e., of lists showing those granted access to administrative data ○ Periodic reviews of access privileges to ensure that access is still warranted ○ Timely removal of access as needed, e.g., for employees whose job responsibilities have changed, employee terminations ▪ Define and/or describe each data element for which responsibility is assigned ▪ Understand how those data elements functionally interrelate ▪ Maintain, document and communicate data definitions, descriptions and interrelationships to authorized administrative data users ▪ Train and assist authorized administrative data users in the function and interpretation of the data ▪ Promote the security of the data for which responsibility is assigned and report any violation or abuse to the Data Custodian, the Vice President and CIO, or the Director of Administrative Computing Services |

| | |
|--------------------------------|---|
| Administrative Data Users | <ul style="list-style-type: none"> ▪ Complete appropriate forms, as delineated in established University procedures or practices, or as deemed necessary by the responsible Data Custodians ▪ Abide by the University IT policy that prohibits account/password sharing ▪ Access and use University data only to fulfill assigned University duties ▪ Ensure the privacy of data by viewing and storing data and the information derived from data securely ▪ Release data and the information derived from data only to support the normal functions of their administrative and academic duties ▪ Administrative data users may not release University data or information derived from that data in any manner which duplicates a function reserved by a University Data Custodian without the permission of the Data Custodian. |
| Dean, Administrative Unit Head | <ul style="list-style-type: none"> ▪ Deans and Administrative Unit Heads are the Data Custodians for non-central University administrative data generated and stored in their areas. ▪ When University administrative data are downloaded to an administrative office, decanal office or department, the responsibility for implementing, monitoring and enforcing University data access policies resides with the Dean or Administrative Unit Head. |

Enforcement

The University will regard an unauthorized attempt to use or the unauthorized use of data as an extremely serious violation of University policy. The University may temporarily suspend, block, or restrict access to information and network resources when necessary to protect the integrity, security, or functionality of University resources or to protect the University from liability. Violation may also result in criminal prosecution under Article 156 of the New York State Penal Code.