# INFORMATION SECURITY: DATA ACCESS AND SECURITY POLICY

**Category:** Information Technology
**Responsible Office:** Computing & Information Technology
**Responsible Executive:** Chief Information Officer

**Date Established:**
**Date Last Revised**: 9/18/2015
**Date Posted to Library:** 9/2/2011

## Summary

This policy defines the data management environment and assigned roles and responsibilities for protecting UB's non-public information from unauthorized access, disclosure, or misuse. It is the responsibility of every University employee who accesses non-public data and information to secure and protect that data.

Many federal and state laws regulate the collection, handling and disclosure of University administrative data[1], including the Family Rights to Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Federal Privacy Act of 1974, New York State laws including the New York State Personal Privacy Protection Law, and Payment Card Industry regulations.. Exposure of confidential data through improper disclosure or security risk is a violation of these laws, and can result in the institution's incurring legal liability, financial liability, loss of reputation, and loss of trust. In addition, New York State has enacted an Information Security Breach Notification Act which requires all state agencies to notify individuals if there is a security breach involving their *restricted confidential data*[2].

The use of mobile computing devices (e.g., laptops, PDAs, cell phones, USB drives) increases the vulnerability of university electronic data to theft and unauthorized disclosure and mandates additional requirements for securing non-public data as set forth in Standards for Securing Regulated Private Data.

This policy has been amended to define additional roles and responsibilities with respect to access to enterprise-wide University summary/aggregate data. Enterprise-wide data includes, but is not limited to, financial, human resource, research, space, advancement, student, and enrollment data.

## Policy

Access to University administrative data[1] 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 non-public data. All University data must be classified by data trustees according to one of the classification levels below, and non-public information must be consistently protected throughout its life cycle (from its creation to its destruction) in a manner corresponding to its sensitivity and/or criticality regardless of where it resides, what form it takes, what technology is used to handle it, and what purpose it serves.

The President, Provost, and Executive Vice President are the data owners or custodians of University data, with the authority to delegate access to aggregated/summary enterprise-wide

University data to eligible personnel and to their office staff as they deem appropriate. Senior Management, defined as the President, Provost, Executive Vice President, Vice Presidents, Associate Vice Presidents, Vice Provosts, and Deans, are eligible for access to enterprise-wide University aggregate/ summary data, providing the oversight to see that access is granted as needed and revoked when no longer needed. Sensitive and regulated data, including Social Security Numbers, credit/debit card numbers, and NY State drivers' license/non-drivers' identification numbers, may not be included in enterprise-wide aggregate/summary data.

### Reason for Policy

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

## Classification of Institutional Data

- Data Classification Standard (Updated 6/7/2010)

| Term | Definition |
|---|---|
| Senior Management | The President, Provost, Executive Vice President, Deans, Vice Presidents, Vice Provosts, and Associate Vice Presidents are designated as Senior Management<br>• Senior Management members are eligible for access to enterprise-wide University summary/aggregate data.<br>• The President, Provost, and Executive Vice President are authorized to delegate access to enterprise-wide summary/aggregate university data to eligible personnel (the members of the Senior Management group) and to their office staff as deemed appropriate. |
| Data Custodian (Owner) | 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.<br>Data Custodians include the Provost, Vice Provost and Dean of Undergraduate Education, Executive Vice President for Finance and Operations, Associate Vice President for Information Technology, Vice President for Research, and Vice President for Student Affairs. |
| Data Trustee (Access Administrator) | 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. The Data Trustee for University enterprise-wide summary/ aggregate data is the Information Security Officer. |
| Administrative Data Users | An administrative data user is any person who has been granted authorization by a Data Custodian or 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 a "user agreement" outlining their responsibilities, before receiving access to data. |
| Functional Areas of University Administrative Data | The eleven functional administrative areas of InfoSource data are: Admissions, Athletics, CASA, Email Addresses, Employee, Financial, Graduate School, Information Technology, Inventory, Student Services, and UBF Financial. |
| University Administrative Data | University Administrative Data include centrally-stored data as well as administrative data generated and stored in University departments and decanal areas. This policy applied to administrative data in any form: hard copy/printed reports, as well as electronic data. |

The following definitions apply to terms used in this policy.

## Administrative Functional Areas and Their Respective Data Trustees

| Data Subject Area | Data Trustee | Telephone |
|---|---|---|
| Admissions | Associate Director of Admissions | 645-6423 |
| Athletics | Senior Associate Athletic Director | 645-3453 |
| CASA | Senior Assistant Vice President, OIA | 645-2791 |
| Email Addresses | Information Security Officer | 645-3582 |
| Employee (State or RF) | Director, Information Resources HR | 645-5000 ext. 1279 |
| Financial Data | Director, Budget Services | 645-5000 ext. 1351 |
| Graduate School | Assistant Dean | 645-2939 |
| Information Technology | CIO and Associate VP for IT | 645-7979 |
| Inventory | Director, Inventory Services | 645-5000 ext. 1110 |
| Student Academic Records | Senior. Assoc. Vice Provost and Director of Student Academic Records and Financial Services | 645-2450 |
| UBF: Financial | Executive Director, UBF | 645-3011 |
| Alumni | Vice President for University Advancement | 645-2925 ext. 150 |
| Extracted Proprietary RF Data | Executive Vice President for University Support Services or designee acting as Operations Manager | 645-2901 |
| HIPAA Compliance | Director, UB HIPAA Compliance | 829-3172 |
| Other University Administrative Data | Appropriate Dean or Department Head | |

### Roles and Responsibilities

| Area | Responsibility |
|---|---|
| The President, Provost, Executive Vice President | Data Owners/Custodians responsible for delegating access to enterprise- wide University data to those eligible (the members of the Senior Management group) and to members of their office staff they deem appropriate. |
| Associate VP for IT | Responsible office for campus IT strategic plans and IT policies |
| Information Security Officer | Responsible for Information Security at University at Buffalo. Security incidents are reported to the ISO. |
| Data Custodians | Manage University information resources; ensure that access to data is granted only 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 this policy |
| Data Trustees | Data trustees classify data in their functional areas; develop and maintain clear and consistent procedures for access to university administrative data; grant and revoke access; maintain an audit trail, i.e., lists showing those granted access to administrative data; periodically review access privileges to ensure that access is still warranted; remove access in a timely manner for employees whose job responsibilities have changed; promote the security of the data in their subject areas. |
| Administrative Data Users | It is the responsibility of every user of UB's non-public data to comply with this policy; to secure any non-public data and to comply with the *Standards for Securing Sensitive and Regulated Data* |

## Procedure

This policy serves several purposes: it establishes a data classification scheme based on sensitivity level and legal requirements; classifies University administrative data into 14 functional areas and assigns the data trustees for each area; and sets forth the responsibilities of data custodians, data trustees, and administrative data users. Anyone who possesses or has access to University administrative data, electronic or otherwise, is responsible for securing and protecting the data.

Therefore, those who request, use, possess, or have access to University administrative data must agree to certain guidelines. Examples of these guidelines are found below as well as on the User Agreement completed by individuals seeking access to data. Data trustees will issue detailed guidelines for each functional area.

1. Access to non-public University information is granted and revoked by data trustees. Access is granted only to those with a legitimate business need for the data.
2. Employees and their supervisors will be asked to complete and sign a user agreement, the Access to University Information Form, confirming that they will follow security guidelines before being given access to non-public University information.
3. Access to Social Security Numbers in UB InfoSource is highly restricted and granted only to a small number of employees with a specific legal or business need. Requesting access to SSNs in UB InfoSource requires the completion of an additional form, stating the legal statute and/or business need. All SSN access requests are reviewed by data trustees and the Information Security Officer.

4. 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.
5. Employees with access to *confidential restricted data* are required to secure the data and follow standards delineated in: Standards for Securing Private and Regulated Information Such as SSNs, Credit/Debit Card Numbers
6. Extracts of data, data feeds, and data within Shadow Systems shall have the same classification level and utilize the same protective measures as the same data in the Systems of Record.
7. Computer systems used to support data will be required to adhere to the specific protective measures for the classification level.
8. Unencrypted Confidential Restricted data cannot be stored on mobile devices, including laptops, USB drives. Please see *Standards for Securing Private and Regulated Information Such as SSNs, Credit/Debit Card Numbers* for additional information about protecting the confidentiality of personal private information.

### Applicability of Policy

This policy applies to all University data regardless of its medium and/or form, and to all those who handle University information (faculty, staff, students, third party contractors, and any others).

### Policy Review and Update

The Associate VP for Information Technology or his designee will periodically review and update this policy as needed. Questions concerning this policy should be directed to the Office of the Associate VP for Information Technology.

### Compliance

Violations of this policy will result in appropriate disciplinary measures in accordance with University policies, applicable collective bargaining agreements, and state and federal laws.

## Contact Information

Information Security Officer
517 Capen Hall
University at Buffalo
sec-office@buffalo.edu
(716) 645-3582

## Related Information

**University Documents:=**
Standards for Securing Regulated Private Data
Social Security Number Policy

**Other Documents:**
New York State Information Security Policy

[1] University data are items of information that are collected, maintained, and utilized by the University for the purpose of carrying out institutional business. Research data, scholarly work of faculty or students, and intellectual property are not covered by this policy.

[2] NY State requires that state entities notify NY State residents if their private information has been acquired by a person without valid authorization. Private information is defined as unencrypted personal information and one or more of the following: social security number; driver's license number or non-driver ID; account number, credit or debit card number and security code which permits access to an individual's financial account.