INFORMATION SECURITY DATA ACCESS

policy.fredonia.edu

Effective Date	*November 18, 2019*
Policy Number	*TEC-PL-102.2*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Security Office (ISO)*
Next Review Date	*November 18, 2024*

I. REASON FOR POLICY

The State University of New York at Fredonia (*"Fredonia"*) is committed to the confidentiality, integrity, and availability of institutional data. Many federal and state laws regulate the collection, handling and disclosure of Fredonia data, 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 Data Security Standards. Exposure of Fredonia's data through improper disclosure or security risk is a violation of these laws, and can result in the University's incurring legal liability, financial liability, loss of reputation, and loss of trust. In addition, New York State has enacted the Information Security Breach Notification Act which requires all state agencies to notify individuals if there is a security breach involving their restricted confidential data.

II. POLICY STATEMENT

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

Research data, scholarly work of faculty or students, and intellectual property are not covered by this policy.

ROLES AND RESPONSIBILITIES

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 non-public data. All university data must be classified by data trustees according to one of the classification levels in the Data Risk Classification Policy, 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 as specified in the Data Risk Classification Policy.

Role	Responsibility Definition
President	The President is Fredonia's Data Owner and is ultimately responsible for the integrity, availability and confidentiality of institutional data. He or she is responsible for delegating access to enterprise-wide university data to those eligible (members of the Executive Cabinet) and to members of their office staff they deem appropriate. The Data Owner or designee, will approve the Data Trustees.
Associate Vice President for Information Technology/CIO	Responsible office for campus IT strategic planning, operations and IT policies
Information Security Officer	Responsible for Information (Cyber) Security at the State University of New York at Fredonia. Security incidents are reported to the ISO.
Data Trustee	A Data Trustee has oversight responsibility for the portion of University Data that is related to the business functions managed, administered or run by the units and personnel who report to him or her. Each Data Trustee will assign one or more Data Custodians to be responsible for data management within the Data Trustee's department. Data Trustees include the following: ● Provost ● Vice President for Finance and Administration ● Vice President for Advancement, Engagement, and Economic Development ● Vice President for Enrollment and Student Services Responsibilities include: ● 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 • Assign and approve Data Stewards
Data Stewards	A Data Steward, assigned and approved by a Data Trustee, has the primary responsibility for the accuracy, privacy and security of a designated set of University Data. All University Data must have a specific Data Steward assigned. University-specific data that need special security or privacy considerations will be defined further by the designated Data Trustee and Data Steward. Data Stewards are responsible for the following: • Categorize the data in accordance with the Data Risk Classification Policy • Develop and maintain clear and consistent procedures for access to university administrative data • Grant and revoke access in accordance with the access procedure in this policy • 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 • Ensure that Administrative Data Users apply applicable Data Retention Policies • Report security incidents to the Information Security Officer
Administrative Data Users	An administrative data user is any person who has been granted authorization 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.

	Administrative data users must complete and sign a "Confidentiality Agreement" outlining their responsibilities, before receiving access to data. Every user of Fredonia non-public data is responsible for ● Complying with this policy ● Securing non-public data in accordance with established security standards ● Complying with the Data Risk Classification Policy ● Completing the required security awareness training ● Comply with applicable Data Retention Policies
Data Functional Category	See the below table.
University Administrative Data	University Administrative Data includes centrally-stored data as well as administrative data generated and stored in university departments. This policy applies to administrative data in any form: hard copy/printed record, as well as electronic data.
Data Custodian	A Data Custodian is an employee of the University who has administrative and/or operational responsibility over Institutional Data. In many cases, there will be multiple Data Custodians. An enterprise application may have teams of Data Custodians, each responsible for varying functions. A Data Custodian is responsible for the following: ● Understanding and reporting on how University Data is stored, processed and transmitted by the University and by third-party agents of the University. ● Understanding and documenting how Fredonia's Data is being stored, processed and transmitted is the first step toward safeguarding that data. Documentation should exist and be made available to the appropriate Data Steward and Information Security Officer for review at anytime. ● Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of Fredonia's Data.

	• Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of Fredonia's Data. • Provisioning and deprovisioning access to Fredonia's Data as authorized by the Data Steward, Trustee, or Owner. • Data Custodians are responsible for provisioning and deprovisioning access based on criteria established by the appropriate Data Steward. • Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of Institutional Data. The Information Security Officer can assist Data Custodians with gaining a better understanding of their data security risks.

DATA FUNCTIONAL CATEGORIES AND THEIR RESPECTIVE DATA STEWARDS

This table classifies university administrative data into 20 functional areas and assigns the data stewards for each area. Anyone who possesses or has access to university administrative data, electronic or otherwise, is responsible for securing and protecting the data in accordance with the Data Risk Classification Policy.

No.	Data Functional Category	Data Steward	Telephone
1	Admissions	Director of Admissions	(716) 673-3251
2	Athletics	Athletic Director	(716) 673-3101
3	Email Addresses	Information Security Officer	(716) 673-4725
4	Employee (New York State and Research Foundation)	Human Resources Director	(716) 673-3434
5	Fiscal Operations	Associate Vice President for Finance and Administration	(716) 673-3109
6	Graduate Studies	Associate Provost	(716) 673-3335
7	Information Technology	Chief Information Officer and Associate Vice President for Information Technology Services	(716) 673-4670
8	Inventory	University Services Director	(716) 673-3257

9	Student Academic Records	Registrar	(716) 673-3171
10	Fredonia Foundation: Financial	Fredonia Foundation Controller	(716) 673-3321
11	Alumni	Director of Alumni Affairs	(716) 673-3553
12	Protected Healthcare Information (PHI) under HIPAA	Director of Youngerman Center	(716) 673-4618
13	Affiliate Business Data	Executive Director, Faculty Student Association	(716) 680-6221
14	Other University Administrative Data	Appropriate Dean or Department Head	N/A
15	FERPA Compliance	Vice President for Enrollment and Student Services	(716) 673-3271
16	Student Counseling	Director of Counseling Center	(716) 673-3424
17	Student Health Information	Director of the Health Center	(716) 673-3131
18	Public Safety and Security	Chief of University Police	(716) 673-3333
19	Student and Staff Housing	Director of Residence Life	(716) 673-3341
20	Student Financial Aid Records	Director of Financial Aid	(716) 673-3253
21	Title IX Information	Chief Diversity Officer	(716) 673-3358

A request to change an entry in this table must be submitted in writing (email is acceptable) as follows:

- A Data Functional Category change must be requested by the designated Data Steward or Data Trustee.
- A Data Trustee change will be handled by the President.
- A Data Steward change must be requested by the designated Data Trustee.

DATA ACCESS STANDARD

Those who request, use, possess, or have access to university administrative data must follow the below Cabinet approved guidelines. Data Trustees will issue detailed guidelines for each functional area where applicable.

1. Access to non-public university information is granted and revoked by Data Stewards or their approved designee.
2. Access is granted only to those with a legitimate business need for the data.

3. Before access to data is granted, the requester must complete the Fredonia Confidentiality Agreement.
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 will be required to complete annual Security Awareness training facilitated by the Human Resources department.
6. Access to Restricted Data (Level III) is granted only to a small number of employees with a specific legal or business need. All requests must be made in writing approved by the appropriate supervisor and submitted to the appropriate Data Steward.
7. Any access to Restricted Data (Level III) by a third party must be approved by the Information Security Officer or designee.
8. Extracts of data, data feeds, and data within shadow systems shall have the same risk classification level and utilize the same protective measures as the same data in the systems of record. All shadow systems will be disclosed to the appropriate Data Trustee and the Information Security Officer.
9. Computer systems, without regard to ownership, used to access University data will be required to adhere to the appropriate minimum data security requirements for the risk classification level as set forth in the Data Risk Classification Policy.
10. All access control requests and approvals for University data will be formally documented in the Information Technology Services Incident Management (Ticketing) System whenever possible or the appropriate business system.

COMPLIANCE

Violations of this procedure may result in disciplinary measures up to and including termination in accordance with University policies, applicable collective bargaining agreements, and state and federal laws.

III. RELATED DOCUMENTS, FORMS AND TOOLS

There are no documents, forms or tools related to this policy.

IV. DEFINITIONS

TERM	DEFINITION
Data Functional Category	Includes University data categorized based on its primary use and functionally under the stewardship of a particular department, division or affiliated entity.
University Administrative Data	Includes centrally-stored data as well as administrative data generated and stored in university departments and decanal areas. This procedure applies to administrative data in any form: hard copy/printed reports, as well as electronic data.
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.

V. CONTACT & ENFORCEMENT

ROLE	CONTACT	PHONE	EMAIL - Website
Responsible Office	Information Security Office (ISO)	(716) 673-4725	security@fredonia.edu
Enforcement	Information Security Office (ISO)	(716) 673-4725	security@fredonia.edu
Policy	University Policy Office	(716) 673-4828	policy@fredonia.edu policy.fredonia.edu