DATA RISK CLASSIFICATION POLICY

policy.fredonia.edu

Effective Date	*November 18,2019*
Policy Number	*TEC-PL-101.2*
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 information important to the University's mission. All University data must be classified into one of three categories described in this policy and protected using the appropriate security measures consistent with the minimum standards for the classification category as described in related information/data security policies.

II. POLICY STATEMENT

Fredonia has classified its physical and electronic data into three risk-based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it. This policy facilitates applying the appropriate security controls to university data, and assists data owners in determining the level of security required to protect data on the systems for which they are responsible.

Please note that the following *Data Risk Classification Categories* and *Risk from Disclosure* levels use the Federal Information Processing Standards (FIPS) 199. The *Minimum Security Standards* use the NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations.

NOTE: The Minimum Security Standards referenced below, will be implemented in accordance with available institutional resources.

This policy applies to all members of the university community, as well as to 3rd parties who handle university data.

Data Risk Classification Category	***Category 3 - Restricted***
Minimum Security	***800-53 High***

Standard	
Risk from Disclosure	**High**
Definition	• 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 is defined using 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), I.T. authentication credentials, and passport numbers. • Restricted data may be 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 affected individuals.
Examples	• Social security number (SSN) • Driver license number • State-issued non-driver ID number • Bank/financial account number • Credit/debit card number (CCN) • Protected Health Information • Passport number • University I.T. authentication credentials • Documents protected by attorney-client privilege

Data Risk Classification Category	***Category 2 - Private***
Minimum Security Standard	***800-53 Moderate***

Risk from Disclosure	***Moderate***
Definition	• Includes university data not identified as Category 3 Data, but includes data protected by state and federal regulations. This includes 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 it is not inadvertently or unnecessarily 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.
Examples	• FERPA-protected data • Gramm-Leach Bliley data • Final course grades, exam questions or answers • HR employment data • Law enforcement investigation data, judicial proceedings data includes student disciplinary or judicial action information • Public Safety information • IT infrastructure data • Collective bargaining negotiation data, contract negotiation data • Trade secret data • Protected data related to research • University intellectual property • University proprietary data • Data protected by external non-disclosure agreements • Inter- or intra-agency data which are not: statistical or factual tabulations; instructions to staff that affect the public; final agency policy or determination • External audit data • University person number • Licensed software • Certain nonpublic Intellectual Property

Data Risk Classification Category	***Category 1 - Public***

Minimum Security Standard	***800-53 Low***
Risk from Disclosure	***Low***
Definition	• Includes university data not included in Category 3 or Category 2 and data that is intended for public disclosure. The loss of confidentiality of this data or the systems containing it would have no adverse impact on Fredonia's mission, safety, finances, or reputation. • 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 the University's website. • Public data has no requirements for confidentiality; however systems housing the data should take reasonable measures to protect its integrity and availability.
Examples	• University financial data or business records available to the public • Approved meeting minutes • Administrative process data • Data about decisions that affect the public • Other university public data • General access data, such as that on unauthenticated portions of the institution's website

All university data stored on university resources or other resources where university business occurs must be classified into one of the three categories. Based on the data classification, data owners, trustees, custodians, and users are required to implement the appropriate minimum security standards set forth by the Information Security Committee for protecting the data. The standard for protecting the data becomes more stringent as the risk from disclosure increases.

Compliance with the *Data Risk Classification Policy* and the corresponding minimum security standards should be incorporated into business processes to ensure data is properly secured. 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. University data stored on non-university IT resources must still be verifiably protected according to respective minimum security standards.

III. RELATED DOCUMENTS, FORMS AND TOOLS

There are no related documents relevant to this policy.

IV. DEFINITIONS

There are no definitions relevant to 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