DATA RISK CLASSIFICATION POLICY

Category: Computing and Instructional Technology
Responsible Office: Chief Information Officer

Date Established: 11/01/2017
Date Posted to Library: 02/27/2018

POLICY SUMMARY

Buffalo State College is committed to the confidentiality, integrity, and availability of information important to the college mission. All college 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.

POLICY

Buffalo State 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 college 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.

DATA IS CLASSIFIED INTO THREE CATEGORIES

Data Risk Classification Category	Category 3 - Restricted
Minimum Security Standard	NIST 800-53-III High
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, college policy adds protected health information (PHI), IT 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 college to disclose any breach of the data to 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 and Visa numbers ● College IT authentication credentials ● Documents protected by attorney-client privilege
Data Risk Classification Category	Category 2 - Private
Minimum Security Standard	NIST 800-53-II Moderate
Risk from Disclosure	Moderate
Definition	● Includes college 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	Data of the following types that are specifically exempted from disclosure under FOIL: ● FERPA-protected data ● Gramm-Leach Bliley data ● Law enforcement investigation data, judicial proceedings data including student disciplinary or judicial action information ● IT infrastructure data ● Collective bargaining negotiation data, contract negotiation data

	• Trade secret data • Protected data related to research • College intellectual property • 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 • College person number (BannerID, SUNYID, NYS Employee ID) • Licensed software • Intellectual property
Data Risk Classification Category	Category 1 - Public
Minimum Security Standard	800-53 Low
Risk from Disclosure	Low
Definition	• Includes college 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 Buffalo State'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 institution'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	• Network usernames • Information authorized to be available on or through the college's website without network authentication • Policy and procedure manuals designated by the owner as public • Job postings • College contact information not designated by the individual as "private" • Information in the public domain • Publicly available campus maps • External reporting data

All college data stored on Buffalo State resources or other resources where college business occurs must be classified into one of the three categories. Based on the data classification, data trustees, stewards, custodians, and users are required to implement the appropriate minimum security standards 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 college information technology (IT) resource as a result of incidental personal use is not considered college data. College data stored on non-university IT resources must still be verifiably protected according to respective minimum security standards.

RESPONSIBILITY

This policy applies to all members of the college community, as well as to third parties who handle college data.

RELATED DOCUMENTS

Buffalo State Guidelines for Storing and Transmitting College Data

CONTACT INFORMATION

Resources for Information, Technology
and Education (RITE)
Cleveland Hall 515
1300 Elmwood Avenue
Buffalo, NY 14222

Phone: (716) 878-3694
Website: http://RITETeam.buffalostate.edu
E-mail: RITE@buffalostate.edu

APPROVAL

President's Cabinet, 01/30/2018