SUNY Buffalo State
Guidelines for Storing and Transmitting College Data

SUMMARY

Under the SUNY Buffalo State Data Risk Classification Policy, all college data must be classified into one of three categories and protected using the appropriate security measures consistent with the minimum standards for the classification category. These guidelines provide direction regarding the storage and transmittal of campus data as specified in the Data Risk Classification Policy.

GUIDELINES

DATA TYPE	EXAMPLES	CAMPUS NETWORK STORAGE (RITE Provides Backup)		CLOUD STORAGE (Vendor Controls Data Availability)				LOCAL STORAGE (You Provide Backup)		
		Personal U: Drive	Dept. Share or Other Network Folder	Shared via Buffalo State email (O365 / Outlook)	Campus-Specific Contract in Place (All O365 / OneDrive)	NO Campus Contract in Place (WuFoo, DropBox, etc.)	Personally Acquired / Maintained Cloud Services	Campus Desktop Hard Drive (C:)	Campus Laptop / Portable Storage	Personal Laptop / Other Device
Restricted: High Risk (See note 1)	• Reports/documents containing SSN or driver's license numbers • Login credentials for any system	YES (1,5)	YES (1,5)	No	No	No	No	YES (6)	No	No
PCI (Credit Card) Data	• Scanned copies of credit cards • Reports of CC payment info	No	No	No	No	No	No	No	No	No
HIPAA (Health) Data	• Doctors' notes • Health Center patient records	No	YES (5)	No	No	No	No	No	No	No
Private: Moderate Risk (See note 2)	• Documentation of physical or electronic security controls • Lists of employees with empID • Reports on ALLSCHOOLS share • Candidate references	YES	YES	No(7)	No	No	No	YES (6)	No	No
FERPA-protected data	• Most reports containing individual student records data	YES	YES	No(7)	No	No	No	YES (6)	No	No
Public: Low Risk (See note 3)	• Lists of award recipients • Reports of directory information (must exclude those with FERPA restrictions) • Minutes of open meetings	YES	YES	YES	YES	YES	YES	YES	YES	YES
Personal: Not work related (See note 4)	• Personal photos or music files • Records of personal transactions	No	No	No	No	No	YES	No	No	YES

NOTES

1. Protection of *Restricted* 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. Access to *Restricted* data should be limited.

2. *Private* data includes college data not identified as *Restricted*, 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*. Private data should not be shared outside the secured locations (e.g. files in the ALLSCHOOLS folder should not be shared with those who do not have access to the folder).

3. *Public* data 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.

4. College policy requires that campus resources be used for official college business only. Non-work-related data should be stored only on personally maintained Cloud services or personally-owned devices.

5. HIPAA protected data may be stored only on network shares that are protected by both network restrictions and folder/file level authentication/authorization or encryption.

6. Private and Restricted data may be stored on a desktop hard drive only temporarily, while reviewing or processing the information.

7. FERPA correspondence to students is restricted to the students' campus email accounts (@mail.buffalostate.edu). Student records data may be shared internally between buffalostate.edu accounts when used in the "legitimate educational interest" of the student, and Restricted or Private data should be encrypted when emailed.

March 2018
Data Governance Committee