DATA ACCESS POLICY

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

Date Established: 04/16/2019
Date Posted to Library: 08/26/2019

POLICY SUMMARY

The purpose of this policy is to establish standards to manage, protect, secure and control college data that will promote and support the efficient conduct of college business. The objective of this policy is to minimize impediments to access of this data while providing a secure environment.

POLICY

Information collected, stored on and accessible by college systems and utilized by college employees and students in support of the educational mission is a vital college asset.

With the oversight of the Data Trustees, Data Stewards and their designated Data Custodians will determine, approve and assign the level of access to institutional systems and data based on employee responsibilities, job functions, or reporting requirements subject to restrictions as imposed by state and federal laws, SUNY policies, and ethical, competitive and practical considerations. The procedures established by Data Stewards to protect the data must not create undue barriers to accessing information.

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. Employees accessing data must adhere to applicable state and federal laws, statutes, and regulations; must comply with protection and control procedures as defined by the institution; and must accurately present the data in any uses.

IMPLEMENTATION AND OVERSIGHT

The Chief Information Officer & Vice President for Enrollment, Marketing, and Communications is responsible for the campus-wide implementation of this policy.

The Data Governance Committee (DGC) is a standing committee appointed by and advisory to the CIO & Vice President for Enrollment, Marketing and Communications. The DGC membership includes a minimum of one representative from each Vice-Presidential unit. On an ongoing basis, the DGC will review policy implementation and recommend policy revisions, when necessary, to the CIO & Vice President for Enrollment, Marketing and Communications. The DGC is also responsible for ensuring that data access procedures across all operational areas are consistent and accessible.

DEFINITIONS, DATA OWNERSHIP AND ACCOUNTABILITY

College Data: The College's data consist of information critical to the mission of the College. Such data are shared and are likely distributed across processing units within the College. Data may be stored in various forms, including but not limited to paper, digital text, graphics, images, sound, or video. The College considers information to be "college data" if it meets any of the following criteria:

at least two organizational units of the College use the data and consider the data essential;

integration of related information requires the data;

the College must ensure the integrity of the data to comply with legal, regulatory and other external reporting requirements;

the data was created or is maintained by a College employee during the course of business;

a broad cross section of users refer to or maintain the data; or

the College needs the data to plan, manage, or audit its operations.

Some examples of college data include student course grades, student and employee payroll and personnel information, buffalostate.edu email systems, and accounting and financial records.

Data Trustees are the highest ranking individuals (typically at the level of Vice President or Provost) accountable for college data. Data Trustees have strategic planning and policy setting authority and are responsible for ensuring that data plans are consistent with and in support of college strategic plans.

Data Stewards are senior management personnel (typically at the level of Associate Vice President, Associate or Vice Provost, Director, or Dean) who have planning and policy-making responsibilities for data in their operational area. The Data Stewards are responsible for overseeing the establishment of data management policies and procedures. They are also responsible for authorizing data sources and elements for their operational area, categorizing the data access type (i.e. public, private or restricted access) and determining who should be authorized to access data. These responsibilities may be delegated to a Data Custodian.

Data Custodians are managers of functional areas (typically at the level of Controller, College Registrar, Director of Admissions or Director of Human Resources) who oversee the capture and maintenance of data for a specific operation. Data Custodians are responsible for making security decisions regarding access to the data under their charge. Their responsibilities also include other activities that may be delegated by a Data Steward.

Data Users are individuals who access College data in order to perform their assigned duties or to fulfill their role in the College community. Data Users are responsible for protecting their access privileges and for proper use of the College data they access. Users will respect the confidentiality and privacy of individuals whose records they access; observe any ethical restrictions that apply to data to which they have access; and abide by applicable laws and policies with respect to access, use, or disclosure of information. All levels of management are responsible for ensuring that all Data Users within their area of accountability are aware of their responsibilities as defined in this policy. Administrative and academic unit heads are responsible for taking the necessary steps to ensure that data

access is terminated (or modified) for employees who transfer to another department within the College or leave employment of the College.

Public data are all data that are not either restricted or judged by the Data Governance Committee to be private or restricted. The accessible data volume should be as great as possible to enable those who need the information to have access. Data should be part of an open atmosphere and broadly available. Under the Freedom of Information Act, public data are subject to disclosure to all Buffalo State employees as well as the general public.

Private data are data determined by the Data Governance Committee to require special procedures for access. Private data may contain elements that are exempt from disclosure under the Freedom of Information Act. Private data may be made available to authorized groups of Buffalo State employees based on their job function.

Restricted data are those data found upon review by the Data Trustees, General Counsel, or the Data Governance Committee to require restrictions on access. Restricted data are protected under law or regulation and therefore exempt from disclosure under the Freedom of Information Act. Restricted data are only available to Buffalo State employees that have a business, research, or educational need to access the data and students who may have a right to their own data under federal law.

PROCEDURE

Data Trustee Assignment

The College determines levels of access to administrative data according to principles drawn from various sources. State and federal laws and regulations provide for restriction of certain types of information. Ethical, competitive and practical considerations also will guide decisions regarding data access. The following table establishes institutional data operational areas and the responsible Data Trustee:

OPERATIONAL AREA	DATA TRUSTEE
Financial (including payroll)	Vice President for Finance and Management
Human Resources Data	Vice President for Finance and Management
Alumni & Development Data	Vice President for Institutional Advancement
Student General Records (including admissions, records, and financial aid)	Vice President for Enrollment, Marketing and Communications
Student Academic Services Records (including advising, appeals, library, academic intervention, and course catalog data)	Provost and Vice President for Academic Affairs
Student Non-Academic Services Data (including medical, housing, counseling, discipline, and athletics)	Vice President for Student Affairs

Information Technology Data	Chief Information Officer
Campus Operations and Facilities	Vice President for Finance and Management

The President, or his/her designee will make decisions regarding division of responsibility where multiple Data Trustees are involved. The Data Trustees will make decisions regarding division of responsibility where multiple Data Stewards are involved. In the event that data exist or are created that fall outside the existing data trustee operational areas above, the executive responsible for the organizational unit will be considered the interim trustee until a permanent assignment can be made.

RESPONSIBILITY

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

RELATED DOCUMENTS

Data Risk Classification Policy

Guidelines for Storing and Transmitting College Data

Guidelines for Maintaining the Security, Confidentiality, and Integrity of Customer Information

Campus Data Stewardship Guide

CONTACT INFORMATION

Information Technology
Cleveland Hall 515
1300 Elmwood Avenue
Buffalo, NY 14222

Phone: (716) 878-3694
Website: https://it.buffalostate.edu
E-mail: itpolicy@buffalostate.edu

REVISION HISTORY

Date of change: 02/03/2020
Brief description of edit: Editorial changes related to divisional reorganization

APPROVAL

President's Cabinet, 04/16/2019