Policy on Data Access

I. Purpose and Scope

Northeastern University recognizes that it is important for the university community to access accurate and reliable university data to fulfill their job responsibilities. At the same time, Northeastern also recognizes the importance of protecting the university’s information assets and preserving the confidentiality and integrity of the data. To provide broad and efficient access to data that appropriately balances data access with the level of sensitivity and attendant risk for different categories of data, this policy establishes internal standards for access to university data that are intended to safeguard data privacy and protect institutional data against misuse or dissemination without proper authorization.

This policy applies to all institutional data, as defined below, that are stored within or transmitted through university information systems. It applies to all members of the university community, including students, faculty, staff, alumni, contractors, vendors, and volunteers in connection with university activities.

II. Definitions

For purposes of this policy,

Data Classification Guidelines – The university’s framework for organizing, categorizing, securing, and sharing institutional data based on the type of data, level of risk, and confidentiality requirements.

Access - A user, system, or process is considered to have access to data if it has one or more of the following privileges: the ability to read or view the data, update the existing data, create new data, delete data or the ability to make a copy of the data. Access can be provided either on a continual basis or, alternatively, on a one-time
or ad hoc basis. Transferring any data from one party to another in any medium is tantamount to permitting access to those data.

**Institutional Data or University Data** - Data that are acquired, created, processed or stored in the performance of university business. Institutional Data does not include data that is the personal property of a member of the University community if such data was acquired or created independent of university business and without university resources. Examples of Institutional Data include student education records, payroll records, human resources records, and enterprise directory records.

**Access Requestor** - University employee who requests access to data which is defined as an individual from the following categories:

- Full or part time hourly or salaried staff or faculty
- University-directed contractor
- Temporary employee

After access is granted the Access Requestor becomes an Accountholder/Data User.

**Accountholder/Data User** - An individual that has been authorized to access data for the performance of his/her job duties.

**Data Custodian** - University employee who oversees data usage and access for their subject area(s). He/she has final approval and authorization for all data related policy decisions and charters new opportunities or initiatives on business/data related issues. A Data Custodian may oversee an area that combines data from several university units.

**Data Steward** - University employee who is responsible for data within a specific subject area. A data steward is a member of senior management who aids in setting the strategic direction for the University's Data Governance Program in areas such as data policies, business process enhancements, data security, and data quality management to safeguard the availability and integrity of institutional data. This is often the head of the university unit that creates or originates the Institutional Data.

**Subject Area** – University line or area of business practice, it may also be known as business area or business domain (ex. Finance, Research, Student, Human Resources, etc.). A Business Domain may consist of multiple functional areas (ex. Functional areas within Finance are: Procurement Services, Accounts Payable, Tax, Treasury Services, Investments, and Accounting).
III. Policy Requirements

A. Data Classification

For university data to be protected throughout its life cycle in a manner consistent with its data type, level of risk, and criticality, Northeastern has adopted Data Classification Guidelines (“Guidelines”). Institutional Data shall be classified in accordance with the Guidelines to identify to users the level of confidentiality, legal requirements, and minimum protections for the data throughout its lifecycle. All institutional data, regardless of where it is stored and maintained, or what purpose(s) it serves, will be classified for the appropriate level of sensitivity, confidentiality, and applicable legal requirements. Extracts from and backups of data shall have the same classification level and require the same protective measures as the source data in the system of record. The Guidelines inform access parameters for each category of data.

B. Access to Data

Individuals may access, use, or store Critical or High Risk (Levels 4 and 3) data only with authorization from the appropriate data custodian, based on demonstration of legitimate business use commensurate with their responsibilities, as well as training where appropriate or required. Requests for authorization should be directly related to business needs and made in accordance with established standards and procedures used by each business domain. Once access is granted, data users are entrusted to exercise due care in using the university’s information, to protect data from unauthorized use, disclosure, alteration, or destruction, and to handle data in accordance with the Guidelines.

B1. Data Custodians are responsible for maintaining the access controls for their areas’ Critical, High Risk and Medium Risk data. Their supervisors and the Data Steward for the subject area are responsible for transitioning the responsibilities as staff turns over.

B2. Data Custodians are responsible for providing guidance and assistance in identifying how to best provide authorized persons access to the university data under their purview required for the requestor’s work, as approved by and agreed to by the account holder’s manager.
B3. Data Administration must retain a record of all access approvals and work with Data Custodians to perform regular reviews of access and remove access to data when no longer required.

C. **Scope of Access Authorization**

Individuals who are authorized to access data throughout its lifecycle must use the data only in a manner consistent with the approved university purpose(s) for which access was granted.

Individuals are not authorized to share data with others who do not have approval to access that same data until explicitly authorized as part of the request for access.

To comply with the minimum security standards for the appropriate data level in the Guidelines, university employees must use university-issued equipment and devices to access Critical, High, and Medium Risk data and must complete all assigned certification courses related to data security and data classification.

Individuals who are granted access to subject area(s) in source systems are generally entitled to have access to the same data in reporting and analytics systems. However, it should not be assumed that if an individual has access to a reporting and analytics systems will automatically have access to the underlying source systems.

If an individual is authorized to provide information to external parties (vendors and other organizations), the individual must work with Information Security and the Office of General Counsel to put appropriate contractual and technical safeguards in place requiring these entities to conform to the Guidelines.

D. **System Administrator Access**

Information Technology professionals and other system administrators who have administrative access to operating systems, databases, or applications being supported as part of their job responsibilities may only use such access in accordance with specific job responsibilities and university policies, and for university business. All such access must be reviewed by their manager and updated or removed as required at the completion of any project or task or after any changes in roles and responsibilities. They must follow the same process for requesting and acquiring access as all other university employees.
E. **Vendor Access**

Proposed access to institutional data by external parties shall be reviewed in advance by the Office of Information Security (in consultation with the Office of the General Counsel, as appropriate), limited to the least amount of data necessary to fulfill the university’s specific business purpose, and governed by individual contractual agreements that include non-disclosure and data safeguarding requirements.

Contractors performing work on behalf of a vendor should have minimal access and should have terms in the master agreement with the university that define their responsibilities and data access.

F. **Access for Research Purposes**

University data related to research falls into two categories:

- administrative research data that enables the tracking of research efforts (e.g. proposals, awards, budgets, expenditures)
- academic research data that is the input or output of the research (e.g. test results, data analytics, subject databases).

Administrative research data is included in the definition of Institutional Data and is covered by this policy.

The second category, academic research data, shall be governed by other Northeastern policies as well as the terms of any contract or grant, data use agreements, and IRB-approved protocols. Researchers must follow Northeastern policy and guidance issued by NU-RES Research Compliance for any academic research data that is defined as Controlled Unclassified Information (CUI) or may be subject to Export Controls. For more information please see https://research.northeastern.edu/research-compliance/.

G. **Access Reviews**

Periodic data access reviews for all constituencies will be conducted by Data Administration with consultation from Data Custodians and managers to revalidate that access remains appropriate. An individual’s access to data must be revoked promptly when it is no longer necessary for performance of their university-related duties. All data users must immediately report any suspected unauthorized access, compromise, or loss of data to the Office of Information Security.
H.  **Training**
All new employees are required to get trained on data security and data classification before accessing Institutional Data.

I.  **Non-Compliance**
Inappropriate access, use or disclosure of critical, high, and medium risk university data outside the scope of applicable authorization may be subject to disciplinary measures up to and including termination (or in Canada termination for cause).

IV.  **Additional Information**
The Data Classification Guidelines apply to all Institutional Data, regardless of format, and irrespective whether such data is contained in a defined “university record”. See [Policy on Confidentiality of University Records and Information](#).

**Contact Information**
To report risk to or loss/unauthorized disclosure of sensitive or personal data: [Office of Information Security](#).
For guidance on the Data Classification Guidelines: dataadministration@northeastern.edu
For questions about the policy: dataadministration@northeastern.edu
For privacy-related questions: privacy@northeastern.edu