Northeastern University

Policy on Confidentiality of University Records and Information

GOVERNANCE AND LEGAL

Effective Date: August 1, 2014

Date Revised: March 15, 2021

Supersedes: N/A

Related Policies: Code of Ethical Conduct
Policy on Retention and Disposition of University Records
Policy on Appropriate Use of Computer and Network Resources
HIPPA Policy; My NEU Privacy Advisory

Responsible Office/Department:
Human Resources
Office of Information Security
Office of the Registrar

Keywords: records; private; confidential

I. Purpose and Scope

Northeastern University is committed to maintaining the integrity and security of confidential records and information created, received, maintained and/or stored by the university in the course of carrying out its educational and research missions. This policy addresses the obligations to secure confidential information from unauthorized or unlawful disclosure. It is intended to reflect federal and state law governing privacy and confidentiality of records, as well as university policies and procedures addressing specific categories of records and information, and any applicable international privacy regulations.

This policy applies to all members of the university community, including students, faculty, staff, alumni, and volunteers in connection with university activities, as well as contractors, vendors, consultants and affiliates when performing services for the university. It encompasses all proprietary and non-public information acquired during the course of employment or service to the university, whether paid or unpaid, and regardless whether the information has been documented or inserted into a paper or electronic record. Student records and information are also governed by the Policy on Student Rights Under the Family Educational Rights and Privacy Act.

II. Definitions

For purposes of this policy,

University Records means any documents, data, or other recorded information created or received by Northeastern

employees in the course of university business. These records can exist in any form. Records include paper and electronic documents (including e-mail), microforms, audio and video recordings, databases, and emails. Some examples of records include, but are not limited to, contracts, minutes, correspondence, memoranda, financial records, published materials, photographs, sound recordings, video recordings, drawings and maps, and computer data.

Confidential Records includes without limitation any personally-identifiable student and parent records, financial records (including social security and credit card numbers), and health records; contracts; research data; alumni and donor records; personnel records other than an individual's own personnel record; university financial data; computer passwords, university proprietary information and data; and any other information for which access, use, or disclosure is not authorized by: 1) federal, state, or local law, or any applicable international privacy regulations; or 2) university policy. Most confidential records will fall under Level 3 or 4 ("high" to "critical" risk) of the Data Classification Guidelines, but some Level 2 data might be designated confidential under university or department protocols.

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

Data Custodians are university employees who oversee data usage and access for their business domain. They have final approval and authorization for all data related policy decisions and charter new opportunities or initiatives on business/data related issues.

III. Policy

All members of the university community are required to maintain the confidentiality of business and nonpublic university records and data entrusted to them, except when disclosure is authorized by an appropriate officer of the university or required by law. University records and information may only be used for university purposes. In accordance with federal and state law and university policy, confidential records should never be disclosed without appropriate authorization, and should be maintained and secured according to the following principles:

A. Documents and files (both electronic and hard copy) containing confidential information are to be accessed, used, and disclosed only with explicit authorization and only on a need-to-know basis for the purpose of a job function, contract, volunteer or paid service to the university.

B. Confidential information regarding any individual or entity acquired during the course of employment at, or providing services to, the university must never be divulged to anyone outside of the university without authorization or to anyone within the university except on a need to know basis.

C. Records must be maintained and disposed of according to the university's Data Classification Guidelines, Policy on Record Retention and Disposition, records retention schedule, and accompanying procedures. All data collected, generated, maintained and used by a department or business unit should be assigned a classification level by the data custodian, and the controls appropriate to that level must be followed by data users.

D. Records may only be received, maintained, accessed or transmitted on university resources in accordance with the requirements and safeguards of the Appropriate Use and other applicable policies, regardless of form, medium or device.

E. Upon conclusion of employment or service, or upon request of a supervisor, all originals and copies of confidential records, whether electronic or hardcopy, must be returned to the university and all further access to and use of such information relinquished.

F. If in doubt about whether a record is confidential, the user should treat as confidential any university record which is not already within the public domain, until directed otherwise.

G. The university takes no responsibility for the unauthorized collection, storage or transmittal of third-party information regarding any individual or entity by students, faculty, staff, volunteers or vendors as defined, that if owned by Northeastern would be subject to this policy.

Hiring units are responsible for informing individuals who will be working or volunteering in or for the unit/department of their specific responsibilities under this policy.

IV. Additional Information

Violations of this policy will be treated seriously. Employees' failure to comply with this policy may lead to discipline, up to and including termination. In Canada, violations may result in termination for cause. Student workers employed by the university who violate this policy may be terminated from their jobs and may also face discipline under the Student Code of Conduct. Others covered by this policy may lose the opportunity to contract with, volunteer for, or otherwise provide service to the university. Intentional violations might also subject the violator to criminal or civil prosecution under federal or state laws.

V. Contact Information

Information Technology Services (617) 373-4357
Office of the General Counsel (617) 373-2157
Compliance Department (617) 373-5893
Human Resources (617) 373-2230
HIPPA Privacy Officer (617) 373-4588
Registrar's Office (617) 373-2300
Data Administration (617) 373-3547 (Data Classification Guidelines)