Northeastern

GUIDELINES FOR DATA ACCESS AND USE IN REPORTING ENVIRONMENTS[1]

Version 5.0

March 1, 2019

Northeastern
Office of Institutional Research and Data Administration

[1] This document defines guidelines for data access and usage via Argos and Cognos reporting tools sourced from the Operational Data Store (ODS) and Enterprise Data Warehouse (EDW) respectively

Introduction

Northeastern University recognizes the need for appropriate data access to its employees to enable them to fulfill their job responsibilities. It is also obligated to keep data secure and private to adhere to laws, regulations, and policies. This document will support the mission balancing these essentials in relation to the University's major reporting environments, the Operational Data Store (ODS) and Enterprise Data Warehouse (EDW).

The data in these environments is accessible via following officially supported reporting tools, Argos (ODS) and Cognos (EDW). All members of the University reporting community have an obligation to safeguard university data throughout its lifecycle (Capture, Store, Use, Share, Archive, and Dispose) according to the University Data Classification Guidelines.

Objective

The objective of this document is to outline the level of security, which must be implemented to protect data access and usage in these environments.

Data Access and Usage Guidelines

1. In order to access information sourced from the ODS/EDW, users must obtain proper authorization via the access request form[2]. This review and approval process is facilitated by Data Administration and includes multiple data governance entities such as Data Custodians and Information Technology Services (ITS).[3]

2. Once access is authorized, users are able to access only the information required to perform their job responsibilities.

3. Users are entrusted to use the information retrieved according to the following laws and policies.[i]

Information Provided	Must be in compliance with	NU Link
Northeastern University Policy on Appropriate Use of Computer and Network Resources	Appropriate Use Policy (AUP)	Northeastern University Appropriate Use of Computer and Network Resources Policy
Student Information	Family Educational Rights and Privacy Act (FERPA) Student Data Policies for University Employees and Third-Party Contractors	http://www.neu.edu/registrar/ferpa.html https://registrar.northeastern.edu/article/student-data-policies-for-employees/
Social Security Number (SSN) and Personal Information	Northeastern University Policy on Collection, Handling and Use of the Social Security Number and Personal Information	http://www.northeastern.edu/securenu/wp-content/uploads/2012/02/SSNPI-POLICY_-02262010.pdf

[2] Please refer to the "**Access to University Reporting Environments "section** within Unified Access Dashboard here.

[3] In regards to the ODS, access is granted based upon Job Position. Should the accountholder change his/her Job Position at the University then employee access is automatically terminated and the employee will need to apply the new Job Position. In EDW/Cognos this process is managed manually.

Personal Identifying Information (PII)	Massachusetts Data Protection Laws (MA201 CMR 17.00)	http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
Protected Health information(PHI)	Health Insurance Portability and Accountability Act (HIPAA) of 1996	http://www.northeastern.edu/drc/pdf/HIPAA%20privacy%20practice.pdf
Northeastern University Confidentiality Information	Northeastern University Guidelines of Confidential Data	https://www.northeastern.edu/policies/pdfs/Policy_on_Confidentiality_of_University_Records_and_Information.pdf https://blackboard.neu.edu/webapps/blackboard/content/listContent.jsp?course_id=_127061_1&content_id=_2042464_1&mode=reset
Northeastern University Policy on Retention and Disposition of University Records	Policy on Retention and Disposition of University Records	https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Northeastern University Guidelines to Classify Data by Risk Level and Data Type	Data Classification Guidelines	https://provost.northeastern.edu/app/uploads/sites/2/Data-Classification-Matrix-from-Program-Pilot.pdf
EU General Data Protection Regulation (GDPR)	General Data Protection Regulation	https://www.northeastern.edu/securenu/security-services/gdpr/

4. Reportable data residing in the ODS and EDW is classified into one of the categories by risk level and data type according to the Data Classification Guidelines due to privacy protections mandated by federal, state, local regulations/laws, or University policies.

5. Appropriate procedures on how to safeguard University data must be employed (e.g. data encryption and data masking) to protect it during the following lifecycle stages: capture, store, share, use, archive and dispose as described in the Data Classification web tool.

6. Data is an asset belonging to the University. If it is lost, incorrectly accessed or disclosed, required steps to follow can be found in the Incident Reporting protocols defined in Data Classification tool.

7. The Data Classification risk levels assigned to ODS/EDW data provide guidance for Data Custodians, Data Stewards, Data Administration, and relevant Information Technology Services supporting units in appropriately managing data access controls and for end users/reporters to properly use and distribute data for operations, analysis, and reporting.

Risk Level Classification of ODS/EDW Data[4]

Risk Level	Risk Level Definition	Data Type Definition	Examples
High Risk Level 🔒🔒🔒🔒	Unauthorized public disclosure, alteration, or loss of this data would result in criminal or civil penalties, identity theft, financial loss, invasion of privacy and will have serious adverse effects on the University's reputation, resources, services or individuals.	Data that the university must keep private under federal, state, local or international laws and regulations, industry standards, and/or confidentiality agreements.	• Social Security Numbers • Credit Card Numbers • Medical Records • Passwords
Medium Risk Level 🔒🔒🔒	Unauthorized public disclosure, alteration, or loss of this data would adversely affect the University's missions, reputation, services, safety, finances, resources or individuals.	Data that is not for public consumption. Its handling is based on university-wide policy and/or internal procedures, and takes into account proprietary, ethical, business practice or privacy implications.	• Photos • Non-Directory Student Data • Employee Salary & Evaluations • Unpublished strategic and financial plans
Low Risk Level 🔒🔒	Unauthorized public disclosure or loss of this data would not cause material harm and is unlikely to, but could, pose risk to the University's mission, reputation, services, resources and individuals.	Data that the university could publish by laws and regulations but has chosen to keep confidential. Its handling is based on university or department/unit protocols or procedures.	• Internal memos, reports • Internal operating procedures • Budget plans
No Risk Level 🔓	Public disclosure or loss of this data poses no risk to the University's mission, reputation, services, safety, finances, resources and individuals.	Data that may, or must, be available and accessible to the general public with no expectation for privacy, risk or confidentiality. There are no legal and institutional limitations on its access or use.	• Campus maps • Course Catalogs • FERPA Directory information (except for students who have requested non-disclosure)

[4] Starting from fall 2016 Data was categorized by the classes in the table above. This data will be re-classified into the this classification model no later than July 2019; e.g. Shared Data Standards, Argos/ODS Data Dictionaries and Data Cookbook field definitions, historically developed Business Terms and Concepts

Historical Data Classification in the ODS[5]

Classification Level	Classification Level Description	Examples
Protected Data	Considered the most critical and require the highest level of protection. Should be the default classification for all data. Includes data that the University must keep private under federal, state, or local laws and regulations. Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss and invasion of privacy. May be disclosed to individuals on a strict need-to-know basis only, where law permits.	• Social Security Numbers or Partial Social Security Numbers • Immunization Records • Race and Ethnicity • Disability Records • Student Records • Drivers License Number • Personal Financial Information • Passwords • Financial Account Numbers
Sensitive Data	Private based on its proprietary worth to the University. These data are not generally available to external parties. Because of ethical, privacy or other constraints may not be accessed without specific authorization, or only selective access may be granted. May be accessed only by authorized employees of the university, without restriction, while conducting university business; access restrictions should be applied.	• Date of Birth/Age • Gender • Marital Status • Home Phone Number • Home Address • Payroll Records • Salary information • Specific Donor Information • Aggregate of other (GPA, percentages and counts of race, ethnicity, and disability) • Student Grades
Public Data	Has no legal or other restriction on access or usage.	• Schedules of Classes • Courses Offered

[5] Prior to fall 2016, data was categorized under this model.

	May be open to the University community and to the general public. Some data elements classified as public may have certain dissemination restrictions.	• Degrees Offered • Employee directory Information • Student Directory Information • Degrees Received • Dates of Attendance

Data Safeguarding

1. Authorization for access to data must be requested via the official Access Request Process through the online form[6] and approved by the appropriate accountholder's manager, data domain Data Custodian, Data Administration[7], and then implemented by ITS.

2. Permission to access ODS/EDW sourced institutional data, based on job requirements, will be granted to authorized university staff for legitimate Northeastern University purposes only.

3. In case where a manager's submission is denied by the Data Custodian, the manager can request for a Remediation Session through the ODS/Cognos Access Appeal Form[8].

4. All ODS\EDW sourced data possessed by Northeastern University must have a designated Data Custodian.
   - The Data Custodian acts as an agent in managing the processes of safeguarding institutional data in his/her data domain(s) to ensure that the collection and use of institutional data are in compliance with the laws, regulations, and Northeastern University policies, guidelines and procedures.

   - Data Custodians with the assistance of Data Classification Liaisons, Data Administration, the Data Classification Subgroup, and Information Security will assess risks and threats to data for which they are responsible and accordingly classify the appropriate risk level of institutional data.

   - Data custodians must assure that data users are protecting the University data from unauthorized generation, access, modification, disclosure, transmission, or destruction.

5. Northeastern University staff must report all instances in which ODS institutional data is at risk from unauthorized generation, access, modification, disclosure, transmission, or destruction to Information Security, Data Administration or the Data Custodian. Steps to follow can be found in the Incident Reporting protocols defined in Data Classification tool.

6. Users of data must accept and abide by the "Policy on Confidentiality of University Records and Information" and respect the confidentiality and privacy of individuals whose data they access, observe restrictions that

[6] A project is under way to allow any university employee to initiate an access request for another employee. This section will be updated when this new functionality goes live. It is planned to go live prior to July 2019.

[7] On rare occurrences authorization for executives who report directly to senior VPs and senior VPs themselves can be requested via email and attached to an official access form by Data Administration. This process will be reviewed and adjusted when a new access form goes live.

[8] This form will be revised by July 2019 to include EDW/Cognos in it.

apply to the information they access, and abide by applicable laws and policies with respect to accessing, using and disclosing information.

- ## Compliance

This document exists in addition to all other Northeastern University policies and federal and state laws/regulations governing the protection of university data[9].

Compliance with these guidelines will ensure that uniform safeguards are applied to protect University data throughout the entire data lifecycle (Capture, Store, Use, Share, Archive, and Dispose)

[9] For the full list of the University Policies refer to this link

Document History

Document Version No.	Edited By	Date Approved by DSC	Reason
1.0	Data Administration in conjunction with Information Security	Approved at DSC meeting on 3/9/2012	Original Document
2.0	Data Administration	Approved at DSC meeting on 3/20/2014	Updated internal Student Data link from registrar's Office
3.0	Data Administration	Approved at DSC meeting on 6/19/2015	Updated links on policy page
4.0	Data Administration	Approved at DSC meeting on 10/18/2017	Updated Historical Classifications and added Current Classifications. Updated to reflect ODS Remediation Sessions creation.
5.0	Data Administration	Approved at DSC meeting on 02/07/2019	Updated version to incorporate new Data Classification taxonomy and EDW/Cognos environment