Northeastern

GUIDELINES FOR DENYING ODS ACCESS

Version 3.0

July, 2016

Northeastern
Office of Institutional Research and Data Administration

Table of Contents

Introduction

The Northeastern University Operational Data Store (ODS) contains enterprise reportable data essential to University business. All members of the University reporting community have an obligation to protect University data from unauthorized generation, access, modification, disclosure, transmission, or destruction.

Objective

The objective of this document is to provide guidelines for parties involved in the processing of ODS access requests and, in particular, to aid Data Custodians in their review of these requests and describe valid reasons for denying access.

1.0 Guidelines

The following reasons for denying access have been recommended by the ODS/Argos Security Group and reviewed and approved by the Data Stewardship Council as the appropriate to deny ODS access:

1. Information provided by access request initiator on the ODS/Argos Access Request Form is not sufficient
    - Each text box in Section 3 of the ODS/Argos Access Request Form (Intended Use of Data) must be thoroughly and accurately completed and each question must be answered in full
    - Specific details must be provided in relation to the accountholder's job responsibilities
2. Mismatch between data being requested and what is currently available
    - Request indicates subject area which is not currently available in reporting environment
    - Request indicates dataset which is not currently available in reporting environment
    - Request indicates timeframe which is not currently available in reporting environment
3. Mismatch between data being requested and the stated description of the accountholder's position[1]
    - Requested subject area is not appropriate for consumption by the accountholder as specified in their job responsibilities
    - Requested dataset is not appropriate for consumption by the accountholder as specified in their job responsibilities

Although the above reasons are approved for denying access, in the event an access request is questioned and further investigation becomes necessary, final decisions regarding access requests must still be made by Data Custodians within 5 business days of submission. The only exception to this rule would be the rare occasion where the Data Custodian and manager have agreed to extend this deadline by no more than 30 calendar days, at which point the request will be altered to remove the disputed subject

[1] In the event a Data Custodian believes this to be the case, they must discuss the situation with the accountholder's manager prior to recording a final decision and keep in mind that in relation to FERPA that school officials may access a student's record for the "legitimate educational interest" of that student. An official has a legitimate education interest when they require access to an education record to perform their professional responsibilities related to education. If remediation is required, the University's Compliance unit will take part.

area to allow the form to proceed. Inaction on the part of the Data Custodian will result in escalation to the ODS/Argos Security Group and, if still unresolved, the Data Stewardship Council.

2.0 Glossary

Data Administration: A unit within the Institutional Research Department that provides leadership in the management of institutional data with regard to data policy, governance, access, integration, standards, and quality enabling the University community to make information-based decisions.

Data Custodian: Operational leaders within their functional areas with day-to-day responsibilities of overseeing access to and security of their subject area data.

Data Stewardship Council: Key institutional area leaders, including Data Stewards and other senior management, who have final approval and authorization for all data related policy decisions and charter new opportunities or initiatives for business/data related issues.

ITS Security: Institutional unit which is responsible for overseeing the safety and security of the entire Northeastern University computing environment, including the management and enforcement of ITS security policies.

ODS/Argos Access Request Form: An online form available on Data Administration’s SharePoint site for the university reporting community to request access to the Operational Data Store (ODS) and associated reporting tools.

3.0 Version Control

Document Version No.	Edited By	Date Approved by DSC	Reason
1	Data Administration	Approved by DSC on 11/08/13	Original Document
2	Data Administration	Approved by DSC on 03/11/15	Updated content in section 2