



The State University
of New York

System Administration
Office *of* Institutional Research
and Data Analytics

Data Governance Framework

as of June 28, 2019

Questions? Comments?

E-mail IR@suny.edu

CONTENTS

The Data Governance Framework	2
Guiding Principles	2
Key Points and Guidelines	3
Data Sources Covered by This Data Governance Framework	4
Data Integrity by Data Source	4
1. Unit Record Data From SUNY Campuses Through SIRIS or Other DTS Submissions	4
2. Data From SUNY Campuses – Surveys, Reports, and Ad Hoc Data Requests	5
3. Data From Other Offices at SUNY System Administration	5
4. Data Obtained From Non-SUNY Entities	5
5. Data Obtained From Surveys For Which OIRDA Has Been the Administrator, Coordinator, or Maintains a Repository of Responses	6
Data Access	6
Data Sharing	7
Data Sharing – Memorandum of Understanding (MOU)	8
Data Sharing – non-MOU	8
Procedure for Processing Data Requests	9
Data Security	10
Roles and Responsibilities	11
Director of SUNY OIRDA	11
SUNY OIRDA Staff (general)	11
SUNY OIRDA Staff (specific to SIRIS and DTS submissions)	11
SUNY Campus Staff (in regards to data/survey submissions)	11
OIRDA Functional Area Data Governance Committee	12
OIRDA Functional Area Data Governance Committee Members	12

THE DATA GOVERNANCE FRAMEWORK

In support of the [mission](#) of the State University of New York (SUNY), the SUNY System Administration Office of Institutional Research and Data Analytics (OIRDA) - with support from the SUNY System Administration Office of Information and Technology (OIT) and in collaboration with other System Administration offices and campus institutional research offices - collects, stores, processes, and analyzes a broad and diverse range of data from SUNY's 64 campuses as well as external sources. OIRDA maintains extensive reporting responsibilities to support data-informed decision making across SUNY, to State and Federal authorities, and in response to countless ad-hoc data requests. The office also has responsibility for ensuring that public SUNY data is easily accessible and in user-friendly formats. This Data Governance Framework details how OIRDA manages this data and these responsibilities. Specifically, the Framework:

- Defines data sources,
- Defines data management processes,
- Establishes procedures and protocols for sharing information with internal and external users,
- Outlines procedures for data security,
- Delineates roles and responsibilities for ensuring compliance with framework, and
- Outlines practices that ensure both data quality and integrity.

GUIDING PRINCIPLES

As noted throughout this document, the ethical use of data and commitments to data integrity and privacy are required of all University staff who produce, request, share, or report data. For OIRDA staff, given its scope of work, these commitments are driving principles that shape their work and inform their every action:

Accessibility: Access to data is critical for building a culture of data-informed and data-driven decision-making and to keeping all SUNY stakeholders and the general public informed. Data users should have the ability to access or retrieve the data covered by this policy in a timely manner in accordance with their roles and responsibilities.

Compliance: All data and data requests are processed and handled in accordance with relevant laws, policies, and regulations.

Ethics: SUNY has an ethical responsibility to protect the privacy and confidentiality of every student, faculty, and staff member. Data is used, reported on, and shared in accordance with ethical principles and accepted best practices and to support SUNY's mission and initiatives.

Feasibility: OIRDA addresses reporting needs and data requests that are reasonable, possible, and manageable with available resources.

Integrity: Data shall be collected, maintained, and reported on with reasonable assurances of its consistency, reliability, and accuracy. All data users share the responsibility of maintaining the integrity of the data and data reports.

Security: Data is protected from unauthorized access and improper disclosure. Users are granted different levels of access to data according to their roles and responsibilities.

KEY POINTS AND GUIDELINES

1. This SUNY System Administration Office of Institutional Research and Data Analytics Data Governance Framework operates under the auspices of any overarching SUNY Data Governance Policy.
2. Data security is the shared responsibility of every individual who, in any way whatsoever, interacts with unit record and/or sensitive data.
3. Data integrity is the responsibility of all data users, whether the data be in unit-record or aggregate format.
4. Data requestors should begin by looking to see if the desired information is available online. In many instances, it may already be publicly available via SUNY Fast Facts, OpenNY, IPEDS, etc, or available (to campuses) via BI dashboards. If a request comes in for data that is already available online, the requestor will typically be referred to the appropriate source.
5. Campuses have the primary responsibility for supporting the data/reporting needs of their campus faculty, staff, and students. If a data/reporting request comes in from a campus, it will typically be referred to that campus's IR representative.
6. With respect to student-related records/information managed by OIRDA, data sharing commitments between any SUNY System Administration office other than OIRDA and any outside organization need to be entered into with the written agreement of the Director of OIRDA, regardless of whether or not an MOU is required. Depending on the nature of the commitment, estimates of time and staff requirements may result in a financial charge in order to fulfill the request.
7. Data requests that will be part of grant-funded research projects should include in their budgets appropriate financial compensation for OIRDA's extra work efforts, in an amount to be determined in conjunction with the Director of OIRDA. Only grant-related data requests discussed and agreed upon in advance with OIRDA can be guaranteed to be fulfilled.
8. Any publication or non-SUNY System Administration presentation that incorporates data provided by OIRDA must appropriately cite that the data has been provided or prepared by OIRDA.
9. Data requests should be sent to IR@suny.edu with a subject line of DATA REQUEST and include the following information:
 - Requester Name
 - Organization
 - Nature of request (as detailed as possible)
 - Need for data (to help us ensure you are using the most appropriate data available)
 - Previously received information (if this is a request for updated or related data)
 - Date the data is needed

DATA SOURCES COVERED BY THIS DATA GOVERNANCE FRAMEWORK

1. Unit record data collected from SUNY campuses through SIRIS (SUNY Institutional Research Information System) or other Data Transfer System (DTS) submissions.
2. Data collected from SUNY campuses by other means, including but not limited to, surveys, reports, correspondence, etc.
3. Data obtained from other offices at SUNY System Administration.
4. Data obtained from non-SUNY entities. Examples include NYS Department of Labor (NYSDOL), NYS Education Department (NYSED), National Student Clearinghouse (NSC), and National Center for Education Statistics (NCES).
5. Data obtained from surveys, whether it be unit record or aggregate, for which OIRDA has been the administrator, coordinator or otherwise has responsibility to maintain a repository of responses. Examples include the Student Opinion Survey and the COACHE Faculty Satisfaction Survey.

DATA INTEGRITY BY DATA SOURCE

1. UNIT RECORD DATA FROM SUNY CAMPUSES THROUGH SIRIS OR OTHER DTS SUBMISSIONS

- 1.1. Campuses submit, via a secure portal, student level data including demographic characteristics, academic status and history, course characteristics (including faculty member information), degrees awarded, and financial aid. Data is sent, reviewed, and locked by the campuses on an established schedule.
- 1.2. Data content and format are established by SIRIS data dictionaries, file layouts, and the *System Administration Office of Institutional Research Official Glossary of Terms*.
- 1.3. Campuses are responsible for reviewing their data and addressing any fatal errors or warnings generated by SIRIS business rules (outlined in the SIRIS data dictionaries). Guidance on reviewing data is provided in the *SIRIS Submissions Review Manual*.
- 1.4. Data is reviewed by OIRDA staff before the submission is approved for incorporation into the SUNY Student Data Warehouse. Guidance on reviewing data is provided in *SIRIS Submissions Review Manual*.
- 1.5. All fatal errors must be cleared before a submission can be locked. Depending on their nature and the specific circumstances, warnings may or may not have to be cleared, but all should be reviewed by both the campus and the campus reviewer.
- 1.6. Once data is exported from SIRIS into the SUNY Data Warehouse, circumstances necessitating amendment or correction of the data require communication with the requisite campus. Changing data already in the warehouse should be done rarely and considered an exception to the data collection process. Every attempt should be made prior to locking and approving to ensure the data is complete and accurate, with the final responsibility resting with the campus.
- 1.7. The source of the data should be noted when used in written reports and presentations.

2. DATA FROM SUNY CAMPUSES – SURVEYS, REPORTS, AND AD HOC DATA REQUESTS

- 2.1. OIRDA has several standard surveys that require all or a group of campuses to submit data.
- 2.2. OIRDA may need to request data on an ad hoc basis from campuses in order to respond to a data request.
- 2.3. Campuses are responsible for ensuring the accuracy, completeness, and timeliness of any data submitted to OIRDA.
- 2.4. OIRDA staff responsible for a particular survey or data request review submissions for missing data and for data that does not appear reasonable in comparison to either prior submissions or data from similar campuses.
- 2.5. The source of the data is to be noted when used in written reports and presentations.

3. DATA FROM OTHER OFFICES AT SUNY SYSTEM ADMINISTRATION

- 3.1. For data received from other offices within SUNY System Administration, the responsibility for the accuracy and completeness of the information rests with the originating office.
- 3.2. The OIRDA staff requesting the data must verify that the data received meets the parameters of the original request. Further, the requester is responsible for reviewing submissions for missing data, for outliers, and for data that does not appear reasonable in comparison to either prior submissions or data from similar campuses.
- 3.3. The source of the data is to be noted when used in written reports and presentations.

4. DATA OBTAINED FROM NON-SUNY ENTITIES

- 4.1. For data received from non-SUNY entities, the responsibility for the accuracy and completeness of the information rests with the owner/originator of the data.
- 4.2. The OIRDA staff requesting the data must verify that the data received meets the parameters of the original request. Further, the requester is responsible for reviewing submissions for missing data, for outliers, and for data that does not appear reasonable in comparison to either prior submissions or data from similar campuses.
- 4.3. In order to conduct an analysis with large data sets, it may be necessary to aggregate, make assumptions about missing values, eliminate outliers, mask small cell sizes to protect individuals' privacy, and/or make other adjustments to the data. Any adjustments to data must be clearly documented and made available for subsequent analysis or presentation.
- 4.4. The source of the data is to be noted when used in written reports and presentations.

5. DATA OBTAINED FROM SURVEYS FOR WHICH OIRDA HAS BEEN THE ADMINISTRATOR, COORDINATOR, OR MAINTAINS A REPOSITORY OF RESPONSES

- 5.1. If an outside vendor is used to administer, coordinate, or analyze a survey of SUNY constituents, the vendor's experience with delivering accuracy, completeness, and timeliness must be verified via: (1) a Request for Proposal process, (2) references, or (3) based on past experience with SUNY.
- 5.2. OIRDA is responsible for either coordinating or supporting the administration of the survey to ensure, as much as possible, that processes are carried out in a consistent manner.
- 5.3. OIRDA should ensure potential respondents are aware of: (1) who will have access to responses, (2) whether or not responses will be anonymous, and (3) the purpose of the survey/study.
- 5.4. OIRDA is responsible for maintaining confidentiality if it has been promised to respondents.
- 5.5. In order to conduct an analysis with large data sets, it may be necessary to aggregate, make assumptions about missing values, eliminate outliers, mask small cell sizes to protect individuals' privacy, and/or make other adjustments to the data. Any adjustments to data must be clearly documented and made available for subsequent analysis or presentation.
- 5.6. The source of the data is to be noted when used in written reports and presentations.

DATA ACCESS

OIRDA, with the Office of Information Technology's collaboration and support, is committed to allowing individuals appropriate access to data when needed or desired, while still protecting individuals' privacy and sensitive information.

To that end, there are four different levels of data access:

Level A: Unit-level access with Personally Identifiable Information (PII)

Users have access to the data at the lowest level of detail (e.g., individual student or employee level data) and may view PII. This includes information that is protected by applicable law or statute.

Level B: Unit-level access with restrictions

Users have access to the data at the unit level but with some restrictions. For example, access to PII is generally blocked and some of the access may be limited to the user's own campus information.

Level C: Aggregate-level access

Users have access only to aggregate level data, based on SUNY credentials and/or IT security-granted permissions. In some cases, user's access is restricted to their own campus data. The most common way to access aggregate level data is through dashboards (e.g. BI Dashboards, Tableau Dashboards).

Level D: Public data access

There are no restrictions for accessing public data. Public data is aggregate-level data and is available for public access through the SUNY website, Open NY, and reports that are made public.

The default levels of access recommended by SUNY System Administration OIRDA vary by data source and user type as displayed in Table 1 below. There can be exceptions in which particular users are assigned different levels of access by SUNY System Administration and/or the respective campuses' IT offices.

Table 1: Data Access by Data Source and User					
Data Source	System Admin IR and IT	System Admin Other Offices	Campus IR	Campus Other Offices	Public
1. Data from SUNY campuses – through SIRIS submissions	A	C	B	C	D
2. Data from SUNY campuses - surveys, reports, and ad hoc data requests	A	C	C	C	D
3. Data from other offices at SUNY System Administration	A	C	C	C	D
4. Data from non-SUNY entities	A	C	C	C	D
5. Data from surveys for which OIRDA has been the administrator or coordinator and/or that OIRDA maintains	A	C	B	C	D

DATA SHARING

OIRDA will follow different procedures depending on whether the data is being shared as part of a Memorandum of Understanding (MOU) with outside organizations or it is part of a non-MOU data request.

With respect to student-related records/information managed by OIRDA, data sharing commitments between any SUNY System Administration office other than OIRDA and any outside organization need to be entered into with the written agreement of the Director of OIRDA, regardless of whether or not an MOU is required. Depending on the nature of the commitment, estimates of time and staff requirements may result in a financial charge in order to fulfill the request.

DATA SHARING – MEMORANDUM OF UNDERSTANDING (MOU)

In certain circumstances, signing an MOU with organizations outside of SUNY is necessary before OIRDA shares any data. Typically, an MOU is needed in instances where shared data is at the unit record level and/or contains personally identifiable information (PII). The MOU will delineate the requirements and responsibilities of each party and the terms and details regarding the use and dissemination of the shared data. The objective of data sharing at this level is to inform, evaluate, and/or assess SUNY policies or practices. Any MOU must be developed and executed in collaboration with legal representatives from the participating organizations.

DATA SHARING – NON-MOU

Users can only share data at the same level or lower as the level of access granted to the requestor. The general procedures for requesting data vary depending on who is requesting the data, as outlined below:

Table 2: Data Requests to OIRDA	
Who is requesting the data?	Standard Procedure
Other offices at System Administration	Requests should include as much detail as possible, such as any prior related data, deadlines, and intended use(s).
Campus	The requestor submits a written request to OIRDA.
Media	Media requests are generally received via the SUNY System Administration Communications Office. If a request comes into OIRDA directly from a media representative, it will be routed to the OIRDA Director, who will coordinate with the Communications Office to respond to the request.
Government Officials	Requests from government officials are generally received via the SUNY System Administration Government Relations Office. If a request comes into OIRDA directly from a governmental representative, it will be routed to the OIRDA Director, who will coordinate with the Government Relations Office to respond to the request.
Public	The requestor submits a written request to OIRDA. When information about a particular campus or a particular set of campuses is requested, the requester will likely be referred to the appropriate campus IR contact.
Legal-related from anyone	All legal-related requests, including but not limited to FOIL and subpoenas, should be sent to: Office of General Counsel SUNY York System Administration State University Plaza 353 Broadway Albany, New York 12246

PROCEDURE FOR PROCESSING DATA REQUESTS

First, the data requestor should ensure the data needed is not already available in public format (e.g. SUNY Fast Facts, IPEDS, OpenNY). If the data is available in public format, the requestor will typically be referred to that source.

The data request should include as much specific information as possible. For example, include the desired turnaround time, any previously provided data/tables, and how the information will be used (e.g., budget planning, program assessment, curriculum review/planning, grant proposal). This helps ensure the appropriate data is being supplied and reduces the number of re-requests.

Specifically, a data request should be sent to IR@suny.edu with a subject line of DATA REQUEST and include the following information:

- Requester Name
- Organization
- Nature of request (as detailed as possible)
- Need for data (to help us ensure you are using the most appropriate data available)
- Previously received information (if this is a request for updated or related data)
- Date the data is needed

Once a received data request is deemed feasible, OIRDA will assign the request a priority level, determine datasets needed, estimate time and staff required, and determine if a contract/memorandum of understanding (MOU) is necessary. Priority level will be determined, in large part, based on how well the purpose of the data request fits in with OIRDA and SUNY initiatives, responsibilities, and priorities.

Estimates of time and staff requirements may result in a financial charge in order to fulfill request.

Data requests that will be part of grant-funded research projects should include in their budgets appropriate financial compensation for OIRDA's extra work efforts, in an amount to be determined in conjunction with the Director of OIRDA. Only grant-related data requests discussed and agreed upon in advance with OIRDA can be guaranteed to be fulfilled.

Any publication or non-SUNY System Administration presentation that incorporates data provided by OIRDA must appropriately cite that the data has been provided or prepared by OIRDA.

DATA SECURITY

Data security is the shared responsibility of every individual who in any way whatsoever interacts with unit record and/or sensitive data. In this document, data security responsibilities will be addressed as they apply specifically to OIRDA. However, all data users are expected to follow these same guidelines, as appropriate to data access and usage.

Practices by OIRDA to ensure data security include:

1. OIRDA staff shall use SUNY data only for legitimate business-related purposes.
2. OIRDA staff shall protect their individual login information and not share it with others. If an individual without security access indicates a need for it, s/he will be referred to the appropriate contact for consideration and/or permission authorization.
3. In order to protect sensitive data and information, OIRDA staff shall lock their computer whenever unattended.
4. OIRDA staff shall follow FERPA regulations as put forth by SUNY.
5. OIRDA staff shall be familiar with any specific MOU security requirements pertaining to particular data they may be working with.
6. OIRDA shall encrypt all personally identifiable information (PII) and utilize secure transmission services when sharing/transmitting sensitive data or information.
7. OIRDA staff shall complete any data security or information management training required by SUNY System Administration or required by a SUNY campus or non-SUNY entity in order to access or utilize the respective organization's data.
8. The OIRDA Data Governance Committee shall, at least annually, review levels of access granted to various stakeholders and the data request procedures to ensure the intent and guiding principles of this framework are maintained.

In the event of the loss of data confidentiality, integrity, and/or availability as related to data OIRDA collects, maintains, and/or reports on, the following procedures are to be followed:

1. When an unauthorized disclosure of confidential data, unauthorized modification/destruction of data, or severe disruption of access to IR data systems is discovered, the incident is to be immediately reported to the Director of OIRDA (or designee).
2. The Director of OIRDA (or designee) shall then notify the SUNY System Administration HelpDesk, CISO, and CIO.
3. The Director of OIRDA (or designee) shall follow the breach protocol guidelines indicated in any applicable MOU or contract, as needed and appropriate. This shall be done in collaboration with SUNY Legal.
4. OIRDA shall work with the appropriate offices and personnel to examine the issue and develop steps to prevent future incidents.

ROLES AND RESPONSIBILITIES

DIRECTOR OF SUNY OIRDA

- Assign any responsibilities to OIRDA sub-unit leads as appropriate/necessary.
- Assign data access permissions within OIRDA.
- Provide for any required and/or appropriate security and data access training.
- Maintain and update as needed data collection elements, business rules, and procedures.
- Establish priority for data requests.
- Approve any new OIRDA data requests of campuses and relay the new request to campuses.

SUNY OIRDA STAFF (GENERAL)

- Comply with the policies and procedures related to the appropriate use of SUNY data, as outlined in this data governance framework document.
- Use institutional data only as required to conduct legitimate business activities.
- Ensure and maintain compliance with privacy laws, regulations, and policies, which may vary based on which particular data elements are being considered and/or by different MOUs that may be in place.
- Maintain a secure environment for the use of SUNY data.
- Ensure the accuracy and timeliness of SUNY data in internal and external reporting.
- Encrypt all personally identifiable information (PII) and utilize secure transmission services when sharing/transmitting sensitive data or information.

SUNY OIRDA STAFF (SPECIFIC TO SIRIS AND DTS SUBMISSIONS)

- Adhere to guidelines for SIRIS submissions outlined in the SIRIS Review Manual.
- Assist campuses in resolving fatal errors and warnings.
- Thoroughly review the data submitted by campuses, including warnings, to help ensure the integrity and completeness of data.
- Coordinate with campus and appropriate System Administration staff regarding any updates/corrections to previously submitted data.

SUNY CAMPUS STAFF (IN REGARDS TO DATA/SURVEY SUBMISSIONS)

- Adhere to guidelines for SIRIS submissions outlined in the SIRIS Review Manual.
- Ensure accuracy, completeness, and timeliness of all data submitted to System Administration. This includes thoroughly reviewing any warnings after a SIRIS data submission is free of fatal errors.
- Provide any background, qualifying information, which could explain or add context to the data, when appropriate or requested.
- Encrypt all personally identifiable information (PII) and utilize secure transmission services when submitting data to System Administration.

OIRDA FUNCTIONAL AREA DATA GOVERNANCE COMMITTEE

- Ensure adherence to data governance policies and procedures.
- Identify and resolve cross-functional area data issues.
- Inform stakeholders of important data and reporting issues.
- Resolve conflicts related to the development, use, collection, or reporting of data covered by this framework.
- Review OIRDA Data Governance Framework on an annual basis, or more frequently if needed, and implement changes as necessary and appropriate.

OIRDA FUNCTIONAL AREA DATA GOVERNANCE COMMITTEE MEMBERS

Standing members:

- Director of SUNY OIRDA
- SUNY OIRDA Sub-unit Leads
- SUNY OIT Representative

On-call members participating as needed:

- SUNY Chief Information Security Officer
- SUNY Legal Counsel
- SUNY Compliance Officer
- SUNY Academic Programs Representative
- State-operated Campus Representative
- Community College Representative