CORNELL UNIVERSITY
POLICY LIBRARY

Administrative Data Store Registry

POLICY 5.11

Volume: 5, Information Technologies
Chapter: 12, Administrative Data Store Registry
Responsible Executive: CIO and VP for Information Technologies
Responsible Office: Data Architecture and Analytics
Originally Issued: August 15, 2018

POLICY STATEMENT

Unit data custodians or their delegates are required to register any persistent administrative functional area data repositories.

REASON FOR POLICY

In order to maximize the value of university administrative data, Cornell must document where these resources are stored, how they are secured, and how they can be used in accordance with other related university policies.

ENTITIES AFFECTED BY THIS POLICY

☑ Ithaca-based locations
☑ Cornell Tech campus
☐ Weill Cornell Medicine campuses

WHO SHOULD READ THIS POLICY

- All information technology professionals
- All custodians of university administrative data

MOST CURRENT VERSION OF THIS POLICY

- https://www.dfa.cornell.edu/policy/policies/administrative-data-store

Cornell Policy Library
Volume: 5, Information Technologies
Responsible Executive: CIO and Vice President for Information Technologies
Responsible Office: Data Architecture and Analytics
Originally Issued: August 15, 2018

POLICY 5.11

Administrative Data Store Registry

CONTENTS

POLICY 5.11

Administrative Data Store Registry

RELATED RESOURCES

University Policies and Documents

University Policy 4.7, Retention of University Records

University Policy 4.12, Data Stewardship and Custodianship

University Policy 5.9, Access to Information Technology Data and Monitoring Network Transmissions

University Policy 5.10, Information Security

University Forms and Systems

Cornell University Administrative Data Store Registry (ADSR)
https://adsr.hosting.cornell.edu/

POLICY 5.11

Administrative Data Store Registry

CONTACTS

Direct any general questions about this policy to your college or operating unit administrative office. If you have questions about specific issues, contact the following offices.

Subject	Contact	Telephone	Email/Web Address
Policy Clarification and Interpretation	Office of Data Architecture and Analytics	(607) 255-8256	ODAA-questions@cornell.edu
Criteria for Inclusion of Administrative Data			
Entering or Updating ADSR Data			

DEFINITIONS

These definitions apply to terms as they are used in this policy.

ADSR	Administrative Data Store Registry.
ADSR Operating Unit Delegate	The individual responsible for coordinating the implementation of this policy in the college or operating unit.
Data Steward	Identified vice president or dean responsible for data types as defined in University Policy 4.12, Data Stewardship and Custodianship.
Data Store	A repository for storing, managing, and distributing data sets. It encompasses databases and data warehouses stored on or off premises.
Operating Unit	An organizational unit designated by the president or the provosts, as defined in University Policy 4.2, Transaction Authority and Payment Approval.
Persistent	Continuing to exist or endure over a prolonged period.
System of Engagement	Systems that provide a business service to two or more campus operating units.
System of Record	Non-research data systems that provide administrative information required for the function of additional (integrated) systems.
Unit Data Custodian	The vice president or dean of an operating unit as defined in University Policy 4.2, Transaction Authority and Payment Approval.
University Administrative Data	Steward-regulated data, in any form, stored on or off campus, locally generated or purchased from an external service. For more information, see University Policy 4.12, Data Stewardship and Custodianship.

POLICY 5.11

Administrative Data Store Registry

RESPONSIBILITIES

The major responsibilities each party has in connection with this policy are as follows:

ADSR Operating Unit Delegate	Coordinate the implementation of this policy in his or her college or operating unit. Update, in a timely fashion, the ADSR with any new or changed operating unit data sets. Ensure that administrative data sets for the operating unit are registered accurately in the ADSR. Access the ADSR prior to the development and implementation of any local system to determine whether the desired data to support the local system already exists.
Chief Data Officer, Head of the Office of Data Architecture and Analytics	Ensure accuracy of the ADSR. Make the ADSR available.
Unit Data Custodian	Identify the ADSR operating unit delegate(s) for their operating unit.
Vice President for Information Technologies	Maintain overall responsibility for implementation of this policy.

POLICY 5.11

Administrative Data Store Registry

PRINCIPLES

Overview

Administrative data is a valuable institutional asset of Cornell University. The value of this data can be maximized by increasing its availability and cross-use throughout campus, while maintaining appropriate data security and access controls. Generally, data assets should be made available when a need is identified and appropriate controls are put in place. Toward that end, the university has created a central registry of university administrative data, called the administrative data store registry (ADSR). The ADSR makes this data easier to find, access, identify, understand, use, and share or make available. Specifically, the ADSR:

- Assists in the identification of data gaps, common data needs and data redundancies, and, therefore, opportunities for efficiencies.
- Assists in the identification of opportunities and challenges related to data governance and stewardship.
- Highlights connections of data sources among systems e.g., remediation analysis in cases where owners of downstream applications must be notified of data changes in source systems.
- Identifies the systems of record for various data sets.
- Helps investigators isolate data and data use during a data breach or other problem.

ADSR Operating Unit Delegates

The unit data custodian of each college or operating unit that maintains university administrative data must identify an ADSR operating unit delegate. ADSR operating unit delegates are responsible for coordinating the implementation of this policy for their respective colleges or operating units, and for ensuring that administrative data sets are registered accurately in the ADSR.

POLICY 5.11

Administrative Data Store Registry

PROCEDURES

Determining What Data Must be Recorded in the ADSR

ADSR operating unit delegates are required to register any persistent data sets that contain university administrative data.

Representative examples of persistent data include, but are not limited to, the following:

- Financial management system data warehouse.
- Student information system data warehouse.
- Utility billing system data warehouse.
- Automated systems data – e.g., building energy consumption and systems monitoring.
- University data, combined with local data, in support of college or operating unit business applications.
- University data, combined with local data, used to prepare college or operating unit annual reports.
- Video surveillance data.

◆**Note:** ADSR operating unit delegates should register all administrative data even if they are uncertain if it is steward-regulated.

Entering, Modifying, or Deleting ADSR Entries

The ADSR operating unit delegate is responsible to do the following:

1. Enter new ADSR data via the input/change form at https://adsr.hosting.cornell.edu/.
2. Enter data attributes for all data sets entered into the ADSR.

   ◆**Note:** Required ADSR attributes are listed in the appendix.
3. Submit change or deletion requests via the input/change form at https://adsr.hosting.cornell.edu/, supplying an explanation for the change or deletion.
4. Review, in a timely fashion, entries in the ADSR, and ensure that they are accurate.

Accessing the ADSR

The ADSR operating unit delegate should access the ADSR prior to the development and implementation of any local system to determine whether the desired data to support the local system already exists. If it already exists, the ADSR provides information on whom to contact to request access to this data. If existing data is similar to that desired to support a local system, the ADSR provides information on whom to contact to discuss potential changes, so that the data set can satisfy both existing and new requirements.

The ADSR may be accessed at https://adsr.hosting.cornell.edu/.

POLICY 5.11

Administrative Data Store Registry

APPENDIX: DESCRIPTIONS OF ADSR ATTRIBUTES

The following table lists the attributes for data sets, as they are recorded by ADSR operating unit delegates in the ADSR.

Abbreviation	The shortened name used to refer to the data set.
Access Methods	A list of commonly used methods by which users access the data set.
ADSR Operating Unit Delegate	The individual(s) at the operating unit level with responsibility for registering data sets.
Audience	The business or functional staff members who consume or otherwise use the administrative data set.
BI Solutions	A list of existing Business Intelligence (BI) solutions used by the university to access the data set. Examples include Oracle Business Intelligence Enterprise Edition (OBIEE) and Tableau.
Database Technology	The database technology used by the data set (e.g., Oracle, SQL Server, MySQL).
Data Currency	How often and when the data in the data set is updated.
Data Model	Summarized representation of how the administrative data set is structured. Examples include Denormalized (relational), Relational, Dimensional, Cube, etc.
Data Provenance	A description of the path and transformations of how the administrative data set is sourced from systems of record.
Data Scope	Succinct description of the scope and granularity of the data set (e.g., prior six months, since the installation of a system X, etc.). Note that this includes administrative data assets purchased by the university, created from university systems, or machine generated.
Data Set Summary	A layperson description of the administrative data set that will inform registry users of what the data set consists of and the purpose(s) it serves and whether it is subject to particular regulatory requirements (e.g., HIPPA, FERPA)
Data Source	The system(s) of record for the administrative data set.
Data Steward	Pursuant to University Policy 4.12, Data Stewardship and Custodianship, the identified vice president or dean.
Data Set Business Name	The business name for the data set.
Data Usage	Summarized information about which systems and/or functional areas use or consume the administrative data set.
Familiar Name	The familiar name for the data set – often different from the business name.
Housed By	Where the data set is housed (e.g., on premise or cloud). If on premise, the name of the campus location and if in the cloud, the cloud vendor's name.
Maintained By	The university operating unit that maintains the data set. Often this is not the functional area. Maintenance includes responsibility for data refreshes, data structures, and data representation.
Metadata	Data about the data. The registry identifies if this information is available for the administrative data set in question (i.e., Yes or No).
Operating Unit	Operating units as defined by the university (e.g., CALS, HR, DFA, OVPR, Engineering, Vet, etc.).
Security – Role Based	Yes or No according to whether or not Role Based security is implemented in the data set and, if Yes, a simple description of how this is done.
Security – Row Level	Yes or No according to whether or not Row Level security is implemented in the data set and, if Yes, a simple description of how this is done.
Source Data From	The list of applications and/or databases that source data to the data set.
Table and Column Attributes Available	Yes or No according to whether or not Table and Column attributes (metadata) are available for the data set.
To Request Access	Link to or other information related to requesting access to the data set.