UW-Madison

Restricted Administrative Data Authorization Policy

Policy Summary

The Restricted Administrative Data Authorization Policy governs:

a. authorization to view or use UW-Madison Restricted Administrative Data
b. as authorized by the Data Governance Steering Committee and Data Governance Program

Who This Policy Applies To

The Restricted Administrative Data Authorization Policy applies to all who view, use or access UW-Madison Administrative Data that is classified as Restricted Data.

Rationale

UW-Madison has, as part of its mission, the responsibility to protect data we collect about our students, faculty and staff while at the same time allow for data to be used appropriately to both educate our students and run the operations of the institution.

Unauthorized access to Restricted Data can have significant detrimental effects on individuals or the institution. Restricted Data can be used for fraud and identity theft. Cyber criminals regularly attack computers and networks in higher education institutions. There have been sizeable information security breaches at institutions that resulted in financial impacts of many hundreds of thousands dollars. Those amounts do not account for the loss of reputation and trust that can have a serious ongoing impact on both instruction and research.

Additionally, even though there are federal and state laws, regulations and contracts that regulate the management of different types of Restricted Administrative Data, some of those regulations (i.e. FERPA) leave interpretation and implementation up to the specific institutions which are curating that data. This policy is intended to fill the gaps left by those regulations and laws.

Preventing unauthorized access

To help prevent unauthorized access, the institution needs to clearly define the audience who can view, access and responsibly use Restricted Data. Preventing unauthorized access involves many other safeguards, but knowing who is (and is not) authorized is fundamental.

Reducing the damage from unauthorized access

Obtaining unauthorized use of a user's account is a common way for an attacker to gain access to data. The amount of data at risk is greatly reduced when access to specific data in a specific system is limited to only those authorized users who have a need to know that data on that system. Granting access on a need to know basis is one of the most effective ways of reducing the damage caused by a data breach.

The scope of this policy is limited to Restricted Administrative Data

Restricted Administrative Data is governed by federal and state laws, regulations and contracts, such as the Payment Card Industry Data Security Standard (PCI-DSS) for credit card data, the Gramm Leach Bliley Act (GLBA) for financial data, and the Family Educational Rights and Privacy Act (FERPA) for the portions of a student's record that need to be treated as Restricted Data.

Restricted Administrative data at UW-Madison not only resides in the institution's enterprise transactional systems but also in distributed locations as inputs and outputs of those systems. In those distributed locations it is usually present as a result of specific business processes.

Restricted Research Data is outside the scope of this policy

Restricted Research Data is governed by federal and state laws and regulation such as Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).

Authorization and access to PHI is governed by the policies and procedures of the UW-Madison Health Care component. The three UW-Madison Institutional Review Boards provide oversight for providing access to other types of Restricted Research Data. Thus, existing procedures for managing the access to Restricted Research Data are currently in place and therefore no additional protections are warranted at this time.

Policy Statement

For anyone to have access to Restricted Data, they must be authorized by the appropriate Data Steward, or designee, before they are permitted to view, use or access UW-Madison Restricted Administrative Data.

1. In order to be authorized to view or use a type of Restricted Administrative Data, the user must have one or more of the following as part of their job duties at UW-Madison:
    a. a role in meeting a regulatory or compliance reporting requirement that requires the handling of that data
    b. a role in the management or operation of a business process that requires the handling of that data
    c. a role in the management or operation of an academic process that requires the handling of that data
    d. a system development, system administration, or maintenance role that requires the handling of that data
    e. participation in an instruction improvement initiative that requires the handling of administrative restrictive data

f. participation in a research project that requires the handling of administrative restrictive data

2. Approved procedures must be followed. These include but are not limited to:
    a. procedures by which a user is *authorized* to view or use a type of Restricted Administrative Data, (e.g. SSN's.) The user must receive any required initial and ongoing training in how to handle the data, and must follow any rules that are specific to that data. There may be other initial and ongoing requirements to receive and retain authorization.

3. There must be an approved, periodic audit and review of users who have *access* to Restricted Administrative Data. The audit and review procedures must include a determination of whether or not each user or group of related users still need access to a system, and if not, access must be disabled or removed in a timely manner by the appropriate Data Custodian.

4. The authorized user of Restricted Data may access said data only to fulfill the job duties for which authorization was granted. Further, an authorized user may not access Restricted Data for personal use.

Special Cases

The procedures, training and rules for specific Restricted Administration Data within specific data domains may vary. When these are in conflict, the stricter applies.

Exceptions

Exceptions may be granted by the Data Stewardship Council or designee.

Consequences for Non-Compliance

Failure to comply may result in appropriate action to enforce compliance, and/or denial of access to UW-Madison data or other UW-Madison information resources. In addition:

1. UW-Madison employees who do not comply may be subject to disciplinary action up to and including termination of employment.
2. UW-Madison contractors or associates who do not comply may be subject to penalty under the governing agreement. Compliance with the policy may be a consideration affecting new or renewed agreements.
3. Civil or criminal penalties are possible.

Definitions

Administrative Data: As defined at Data at UW-Madison:

> *"Data that is generated as a result of utilizing enterprise transactional systems, such as student records, employee data, or financial information."*

Restricted Data: As defined by the UW-Madison Data Stewardship Council:

> *"Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a significant level of risk to the University, affiliates or research projects. Data should be classified as Restricted if:*
>
> - *protection of the data is required by law or regulation, or*
> - *UW Madison is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed."*
>
> See https://data.wisc.edu/data-governance/data-classification-examples/ for examples of data elements that are usually treated as Restricted Data.

Restricted Administrative Data then, is Restricted Data that has been generated as a result of utilizing enterprise transactional systems. It includes data that may currently reside in local systems if ultimately the data was generated from an enterprise transactional system. For example, a faculty member has a course roster in an excel spreadsheet. The list of students came from either the LMS or ultimately from the SIS and the faculty member uses the spreadsheet for maintaining grades. This falls within the scope of this policy.

Roles and Responsibilities

Role	Responsibility
Executive Sponsors	The Data Governance Steering Committee has final review and approval of this policy.
Functional Owner	Chief Data Officer under the direction of the Data Stewardship Council, has oversight responsibility for the implementation and maintenance of this policy and associated procedures.
Responsible Party	Data Stewardship Council reviews this policy and associated procedures, makes recommendations to the Executive Sponsors, and may grant exceptions to this policy and associated procedures.
Business Data Custodian	The Business Data Custodian of a type of Restricted Administrative Data, or designee, grants authorization to view or use that type of data,.

Role	Responsibility
Technical Data Custodian	The Technical Data Custodian of a system, or designee, grants access to data on the system to authorized users, and for authorized users,.
User	A user follows this policy and associated procedures to receive and retain authorization to view and use a type of Restricted Administrative Data, and to receive and retain access to specific systems that store or process that data.
Policy Assessment	Chief Data Officer, or designee, under the direction of the Data Stewardship Council, periodically assesses the effectiveness of this policy and associated procedures. The policy is assessed every two years, or sooner. The associated procedures are assessed annually, or sooner.
Policy Contact	Please contact: datagov@wisc.edu

Examples of Uses of Restricted Administrative Data within Scope of This Policy

- A staff member within the department of Academic Planning and Institutional Research submits enrollment totals to the Higher Learning Commission.
- A department administrator is looking at student counts by course for department planning purposes.
- A staff member within University Health Services is scheduling an appointment for a student.
- A staff member within Rec Sports is renting a student a locker and looks up the student within their local application
- A department administrator is tracking Teaching Assistant information for the TA's within his/her department
- A faculty member or lecturer is looking at a class roster.
- An School/College IT application developer is building an application to assist his/her department in tracking information about the students within that School/College
- A Principal Investigator is working on an approved research project that involves UW-Madison students and data collected about those students.

Link to Current Policy

Will be on the data.wisc.edu website

Links to Related Policy

Office of the CIO, Data Classification to Support System Security

Office of the CIO, Responsible Use Policy

Office of the CIO, Restricted Data Security Management Policy

Supporting Tools and Documents

Restricted Administrative Data Authorization and Requirements

Restricted Administrative Data Authorization Procedure [TBD]

Restricted Administrative Data Training, [TBD]

Restricted Administrative Data Handling Rules, [TBD]

Access to Systems Containing Restricted Administrative Data

Accessing Data

References

Data at UW-Madison

Data Classifications

Data Governance Organizational Structure

Review and Revision History

Date	Activity
<TBD>	Effective.
<TBD>	Published.