UW-Madison

Restricted Administrative Data Authorization Procedures

Procedures Summary

The Restricted Administrative Data Authorization Procedures outline the methods by which access can be granted to an individual who will access Restricted Administrative Data.

Who These Procedures Apply To

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

Procedures

1) Authorization and Access Procedures.
   a) In order for an individual to receive permission to access Restricted Administrative Data, he or she must:
      i) Make a request and receive permission from the appropriate Data Custodian in a timely manner. Data Custodians for specific data domains are as follows:
         (1) Student (i.e. Student SSN or student PII) – University Registrar
         (2) Financial (i.e. Credit Card or Financial Acct #s) – Assistant Vice Chancellor for Business Services
         (3) HR (e.g. Employee SSN, Driver License #s) – Director of Human Resources
         (4) PHI – HIPAA Privacy Officer
      ii) Have Undertaken Restricted Data Access Training and passed the Restricted Data Access assessment. (See Section 2)
2) User Acknowledgement Procedures
   a) The user must indicate acknowledgement of receiving the training and understanding of the Restricted Administrative Data Authorization Policy and responsible use of Restricted Administrative Data. The acknowledgement will state the following:
      i) I have read and understand the Restricted Administrative Data Authorization Policy & Procedures.
      ii) I have completed the Restricted Administrative Data Access Training.
      iii) I agree that I will protect Restricted Administrative Data as provided by the Restricted Administrative Data Authorization Policy & Procedures.
      iv) I understand that violation of this agreement may subject me to possible disciplinary and/or legal action affecting my employment. I acknowledge that this form will become a part of my permanent personnel file.

3) Training Procedures

   a) An individual must undertake a comprehensive Restricted Administrative Data Access training prior to gaining access to Restricted Administrative Data.

   b) The Restricted Administrative Data Access Training will be created within Learn@UW

      i) Learn@UW will record who has taken the Restricted Administrative Data Access Training

      ii) The appropriate Data Stewards and Data Custodians will have access to the list of people who have taken the training

   c) An individual must pass the Restricted Administrative Data Access assessment after completing the training.

      i) A user must score 90% or better to pass the assessment.

      ii) If a user does not score 90% or better, he/she must re-take the training and the assessment. The user can retake the training and assessment immediately.

   d) An individual must take a Restricted Administrative Data Access refresher training once every 12 months in order to maintain his/her access to Restricted Administrative Data.

      i) A user will be notified within 30 days of the end of the 12 month period that he/she is expected to re-take the training. The user will need to complete the training prior to the end of the 12 month period in order to maintain his/her access to Restricted Data.

      ii) The refresher training will focus on understanding the core principles of the Restricted Administrative Data Authorization Policy and Principles.

4) Audit Procedures

   a) The appropriate Data Custodian will monitor the list of users who have access to Restricted Data.

   b) The appropriate Data Custodian will review the list of users have access to Restricted Administrative Data and ensure those users continue to meet the criteria necessary to have access.

   c) The appropriate Data Custodian will remove users' access to Restricted Administrative Data if:

      i) The user no longer meets the criteria necessary to have access

      ii) The user is no longer associated with the University of Wisconsin-Madison.

5) Responsible Use Procedures

   a) A user may not share a data set which contains Restricted Administrative Data with others unless they are certain the recipient of the data set also has been granted access to Restricted Administrative Data.

b) A user must store Restricted Administrative Data in environments that have been certified as appropriate to store Restricted Administrative Data.

   i) The Office of the CISO is responsible for certifying environments as appropriate to store Restricted Data.

c) A user may access Restricted Administrative Data only for the approved process for which he/she has been granted access (as outlined in the Restricted Administrative Data Policy.)

   i) Access to the Restricted Administrative Data should be kept to a minimum.

   ii) Access to Restricted Administrative Data for personal reasons is not allowed.

d) Users who have access to Restricted Administrative Data should not respond to Open Records Requests unless doing so is part of their role at UW-Madison.

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 these procedures.

PII: Personally Identifiable Information. Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing data can be considered PII.

PHI: Protected Health Information. The definition of PHI can be found here.

Roles and Responsibilities

Role	**Responsibility**
Executive Sponsors	The Data Governance Steering Committee has final review and approval of these procedures.
Functional Owner	Chief Data Officer under the direction of the Data Stewardship Council, has oversight responsibility for the implementation and maintenance of these procedures.
Responsible Party	Data Stewardship Council reviews these procedures, makes recommendations to the Executive Sponsors, and may grant exceptions to these 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,.
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 these 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 these procedures. The procedures are assessed annually, or sooner.
Policy Contact	Please contact -- datagov@wisc.edu