# Administrative Data Access Provisioning Procedures

**Procedures Summary**

The Administrative Data Access Provisioning Procedures outline the methods by which data, reports or dashboards are segmented into classifications of data domains and how access to those will be granted and maintained

**Who These Procedures Applies To**

The Administrative Data Access Provisioning Procedures applies to the Stewards of our institutional administrative data and to the users of that data.

**Procedures**

1. Access Groups
    a. For each segmented data domain classification, an access group will be created. For example, Restricted Student and Internal HR will be access groups that are created.
    b. Access groups will be populated with members (users) of data, reports, dashboards.
    c. Each data view, report and dashboard will be assigned to one or more access groups by agreement of all relevant data stewards.

2. Data Stewards
    a. Designate Data Custodians for their specific data domain.
    b. The Data Stewards will review administrative data-views, reports and dashboards to determine or confirm:
        i. Data Domain assignments
        ii. Classifications within that assignment
        iii. Access Group assignments
    c. Data Stewards will determine initial membership in the Access Groups within the Data Steward's purview
3. Data Custodians
    a. Data Custodians will review and approve or deny requests for membership within the Access Groups.
    b. Data Custodians will periodically review Access Group membership to de-provision individuals who should no longer have access.
4. Initial Membership to Access Groups
    a. Initial membership to Access Groups will be created by :
        i. Generating a list of users who currently have access to query library queries with data that are in the same data domain and data classification as the Access Group.
            1. Individuals with job titles or functional areas that raise questions about whether or not access to the data is appropriate will be further vetted

by the Data Stewards to determine if membership in the Access Group is warranted.

ii. Generating a list of users who have access to data warehouse data-views with data that are in the same Data Domain and Data Classification as the Access Group will be generated.
    1. Individuals with job titles or functional areas that raise questions about whether access to the data is appropriate will be further vetted by the Data Stewards to determine if membership in the Access Group is warranted.

iii. Merging the two generated lists into one list

iv. Granting membership to the Access Group to the users on the one merged list.

5. Requesting membership to an Access Group
    a. Individuals can request membership to an Access Group by:
        i. Stating their need for access to the data that is provisioned by the Access Group
        ii. Stating their job title / job responsibilities
        iii. Stating their functional area
    b. An individual's supervisor must grant approval for the individual's access to an Access Group
6. Segmenting Data-views, Reports, Dashboards into Data Domain Classifications
    a. Each Data Steward makes a determination of whether the data-view, report, or dashboard falls into that Data Steward's Data Domain. Many reports and dashboards will be cross-functional and fall into multiple Data Domains.
    b. If the data-view, report, or dashboard does fall into the Data Steward's Data Domain, the Data Steward makes a determination of the highest (risk-based) level of Data Classification for that Data Domain in the data-view, report, or dashboard.
    c. Upon making a determination of Data Classification, the Data Steward assigns the data-view, report, or dashboard the Access Group corresponding to the Data Domain and Data Classification.
7. Access to Data-views, reports and dashboards
    a. Access to data-views, reports, and dashboards will be limited to individuals that are members of all Access Groups assigned to a report or dashboard. For example, if a report is assigned the Student Restricted and Faculty & Staff (HR) Restricted Access Groups, then only individuals that are in both of those Access Groups will be able to access the report.
    b. Access groups which have access to data that has been classified at a higher risk-level within the same domain will automatically have access to data at the lower classifications as well. For example, members of the Restricted Financial Access Group will also have access to data-views, dashboards and reports that can be accessed by the Internal Financial Access Group.

**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."*
>
> See https://data.wisc.edu/data-governance/#classifications for a summary of how data is classified into our risk classifications.

APPENDIX A

# Administrative Data Access Provisioning Procedures – Making Operational

1. We will use Data Cookbook functionality to help implement the necessary data collection and workflows for the Provisioning Policy & Procedures. The Cookbook has the ability to capture 'functional areas' and 'data classifications.' It also has a field called 'Access Details.' These three fields, along with the built in workflow functionality make Data Cookbook a centerpiece of operationalizing the policy & procedures.
2. Developers of reports and dashboards will submit documentation of their reports and dashboards through Cookbook. Workflow will be set up so that content is not finalized in Cookbook (or the Portal) until Data Stewards approve the content, thus allowing for their determination of Data Domain, Data Classification, and Access Groups.
    a. We are proposing a regular meeting of the Data Stewards where they review and approve submissions (similar to how the University Curriculum Committee reviews course proposals)
3. Access Groups will be housed in Manifest or InfoAccess (or both.) Access Groups will NetIDs of members, which can be used to automate provisioning in reporting tools, such as Tableau. Users should be provided a way to determine which Access Groups they belong to, through a lookup tool (web app or Tableau viz).
4. Individuals should be able to request membership in an Access Group through the Portal (when the individual sees a report or dashboard of interest that the individual cannot currently access) and through a standalone request form on the data.wisc.edu website.
5. Stewards and developers should be able to request additional Data Domains and/or Access Groups be created to give additional control or granularity to the provisioning structure.