Data Administration Guideline – DMC Access and Roles - EDW User Access Review

Purpose

The UW Data Management Procedures document calls for periodic reviews of the DMC Access and Roles Matrix and corresponding assignment of users to specific roles defined in the matrix. This document outlines processes and best practices for conducting an access review of the roles, and users within those roles, to the UW Enterprise Data Warehouse (EDW).

Overview / Problem Statement

Members of the designated Access and Roles sub-committee of the DMC, in conjunction with appropriate Data Custodians, are responsible for performing regular reviews of the security access standards and guidelines outlined in the DMC Access and Roles matrix. This includes review of users to verify membership in roles and appropriateness of access. The following are best practices for conducting a review of users in roles defined in the DMC Access and Roles matrix for access to data in the EDW.

Administrative Processes and Tools

Designated reviewers will be determined by consensus of the DMC Access and Roles sub-committee. All appropriate Data Custodians (i.e. those responsible for EDW access authorizations) will be notified of who performs the review and when the review occurs. The reviewers will run the Administrative Who Has Access report, located in the Admin folder of the main Enterprise Reporting Services web site, to take a baseline of all users and their role assignments. This report was designed to help reviewers review relevant information about a person to assist in the review. The report can be easily filtered to display users in each of the roles. Each filtered role data set should be saved in a MS Excel worksheet and labeled with an appropriate name and date of the review run. Reviewers should add a notes column, suggested action to take, action taken date and the name of the reviewer taking action, for any changes in access authorizations that may be determined appropriate during the review. Reviewers should review proposed actions to take on any suspicious authorizations with the DMC Access and Roles sub-committee and document actual actions taken that the sub-committee agrees to. Each of the role worksheets should be consolidated into one MS Excel workbook and saved in the appropriate DMC Sharepoint web site at:

https://sharepoint.washington.edu/oim/DMC/STIC/PIC%20Meetings/Forms/AllItems.aspx

The review, and baseline report run, should be conducted in the fall or spring quarters, but not during the summer quarter. There are seasonal bulk changes to employment status of employees that occur during the summer quarter which may result in false positive rows in the Administrative Who Has Access report. The report shows, by each role in the Access and Roles matrix, each users name, their UW netid, date of last ASTRA update, the department name associated with their payroll unit code, and the current employment status indicator. There are a variety of employment statuses possible for an employee. The majority of status indicators will be "Active" but reviewers will find various others including "Inactive", "On Leave", "Retired", and "Separated". These indicators may help a reviewer in verifying appropriateness. Note, there are a variety of reasons in which an employee with a status other than Active may still be valid and appropriate for having access to the data. Many employees who are retired still serve business functions within the UW. Some employees employment status may be temporarily set as Inactive due to seasonal or business cycles and then reactivated later. For guidance on understanding employment statuses reviewers
should consult with HR Data Custodians and review the UW HR policies and procedures website.
http://www.washington.edu/admin/hr/polproc/index.html

Review Guidelines and Criteria

Roles and User Counts

Roles that have broad access to highly sensitive and confidential data (i.e. roles with access to data higher than baseline privileges) typically have fewer users than roles with just baseline access. Reviewers should note the total quantity of users assigned in each role and investigate if the number seems high. The chart below indicates relative number of users per role and a general indication of the units those users are appointed in during the 2011 review. If a users department name in the report varies from the ones typically observed in that role, reviewers should investigate further.

<table>
<thead>
<tr>
<th>Role</th>
<th># Users</th>
<th>Typically Observed Departments</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator</td>
<td>15-20</td>
<td>UW-IT Decision Support Services Only</td>
</tr>
<tr>
<td>Audit</td>
<td>10-15</td>
<td>Internal Audit, CISO only</td>
</tr>
<tr>
<td>Academic Personnel/ HR Analyst</td>
<td>25-30</td>
<td>Central Office HR, Academic HR, EOO Analysts</td>
</tr>
<tr>
<td>Payroll Analysts</td>
<td>20-25</td>
<td>Central department payroll analysts</td>
</tr>
<tr>
<td>Student Fiscal Analyst</td>
<td>20-25</td>
<td>Central student fiscal analysts</td>
</tr>
<tr>
<td>Student Aid Analyst</td>
<td>10-15</td>
<td>Central Student Aid Office analysts</td>
</tr>
<tr>
<td>Institutional Analyst</td>
<td>25-35</td>
<td>Planning and Budgeting, OMAD, SDMO</td>
</tr>
<tr>
<td>Academic Analyst</td>
<td>50-60</td>
<td>UW-IT, Educational Assessment, SDMO</td>
</tr>
<tr>
<td>Chancellors/Deans/Deans Analysts</td>
<td>140-160</td>
<td>Dean, Chancellors, Administrators, Dean’s Office Analysts</td>
</tr>
<tr>
<td>Principal Investigators</td>
<td>5-10</td>
<td>PI’s, or administrators managing grant budgets. Note: this number likely to increase as research data is added to the data warehouse.</td>
</tr>
<tr>
<td>Advisor / Academic Staff</td>
<td>250-270</td>
<td>Advisors and academic support staff in various academic units</td>
</tr>
<tr>
<td>Payroll Coordinator</td>
<td>550-570</td>
<td>Payroll coordinator staff in various academic and administrative units</td>
</tr>
<tr>
<td>Administrative Analyst</td>
<td>400-425</td>
<td>Analysts in a variety of central administrative units (UW-IT, Finance and Facilities, etc.)</td>
</tr>
<tr>
<td>Administrator/Manager/Fiscal Tech</td>
<td>3500-3600</td>
<td>Administrators, managers and fiscal tech specialists in a variety of academic and administrative units.</td>
</tr>
</tbody>
</table>

Large Populations

It is not feasible to review each users access. Reviewers should determine a consistent method for selecting which users to review. For roles with large numbers of users assigned reviewers should discuss with the Access and Roles sub-committee and document the sampling size and method to be used. In addition to random observations reviewers should be reviewing according to the additional practices indicated below.
Multiple Roles and Departments

Some users may have multiple role assignments. The header of the Administrative Who Has Access report shows both unique users and total number of role assignments. During the 2011 review there were 4,744 unique users in 5,403 role assignments. If this general ratio changes significantly it should be documented and discussed with the Access and Roles sub-committee and appropriate Data Custodians. In the report a user may have several rows associated with them indicating multiple role assignments, or multiple department appointments. Users with more than 2 roles assigned or 2 department appointments should be investigated further.

UW NetID and Names

Note that some users may have a UW NetID indicated but no name displays. This may indicate a "Shared UW NetID". These types of UW NetIDs are discouraged but are sometimes necessary for support, testing and training purposes. There are several Shared UW NetIDs used by the systems administrators of the data warehouse for security testing purposes. Refer to DMC Guideline Document #1016 for a complete list. There are also application UWNetsIDs in roles that represent direct system to system accounts setup to extract data out of the EDW on regular schedules. Refer to DMC Guideline Document #1017 for the naming convention and expected usage of these UW NetID accounts.

Using Other ASTRA Authorizations for Context

Reviewers will use the UW ASTRA authorization system to search and verify the access that users have. When searching for users in ASTRA you will be able to see all authorizations to all systems and not just to the data warehouse. The data warehouse roles in ASTRA are named to correspond to the roles in the Access and Roles matrix. Reviewers should review the specific Access and Roles role authorizations in context to other ASTRA system authorizations to help determine appropriateness. For example, users assigned to the "Advisor / Academic Staff" role on the matrix typically have access to EARS (student degree audit system), or users in the "Payroll Coordinator" role on the matrix typically have access to the OWLS (Online Work Leave system)

Retirees and Affiliates

Reviewers should pay special attention to users that have "NOT AVAILABLE" in the Department Name column. This is typically an indication that the person has an "affiliate" relationship with the UW. This is common in the medical services area where a person for example may work in the Fred Hutchinson Cancer Center but has an affiliation with the School of Medicine. Note that some users that have "NOT AVAILABLE" indicator in the department name may have employment indicators in ASTRA set as “Retired but receiving Supplemental Pay”. Many users may also have Alumni and Student Employee affiliations. Affiliated users may have legitimate business responsibilities for the UW and reviewers should refer to associated ASTRA system authorizations for indications of appropriateness to data warehouse role access.

ASTRA Authorization Owners

Note that many users in the "Administrator/Manager/Fiscal Tech", "Administrative Analyst", "Payroll Coordinator", "Advisor/Academic Staff" and "PI" roles are administered by unit authorizers in ASTRA. These roles have been designated as available for decentralized authorizations by unit authorizers. All other roles require centralized approval from appropriate Data Custodian. Centralized authorizations are coordinated and are administered by DMC Standards Implementation Committee (STIC) members, or their
delegates, on behalf of the Data Custodians. In ASTRA the “authorization owners” are the ones responsible for ongoing administration of the access. ASTRA sends authorization owners quarterly emails of employees that have separated, inactive and retired statuses. It is possible due to the timing of the review, and the authorization changes by owners, that reviewers will find separated users access has been removed since the baseline report was run. Users that have an employment status of separtated and have not had ASTRA authorizations removed within that last quarter should be investigated further and possible action taken.

Concurrence / Responsibility

The undersigned concur with recommendations and best practices in this data administration guideline document. They understand the implied risks and benefits outlined in this document and endorse and encourage its use.

Signature
Dean of University Libraries – Betsy Wilson
(Co-Chair of Data Management Committee)

Signature
Assistant Vice Provost Institutional Research and Data Management – Todd Mildon
(Co-Chair of Data Management Committee)

Signature
Director of Enterprise Information Services – Bill Yock
(System Owner for Enterprise Data Warehouse)