TABLE OF CONTENTS

SMAT Overview ........................................................................................................................................... 3
SMAT Roles and Responsibilities .................................................................................................................... 3
SMAT Tips and Support ................................................................................................................................. 3
SMAT Process – The Quick Look .................................................................................................................... 4
  Apply Security Definition ............................................................................................................................ 4
  Submit for Publication ................................................................................................................................. 5
  Review Publication Status ........................................................................................................................... 6
  Help Page ..................................................................................................................................................... 7
  Session Timeout ........................................................................................................................................... 7
SMAT Process - Step-by-Step ......................................................................................................................... 7
  Step 1: SMAT User changes an SDEF ....................................................................................................... 8
  Step 2: SMAT Administrator approves submitted request ......................................................................... 11
  Step 3: SMAT User tests security metadata ............................................................................................. 11
  Step 4: SMAT User submits security metadata for publication ................................................................. 12
  Step 5: SMAT Administrator promotes request to production ................................................................. 12
  Step 6: SMAT Users or Administrator reviews the security metadata published status .......................... 13
  Step 7: Closing your SMAT Session ......................................................................................................... 14
SMAT
Security Metadata Administration Tool
User Guide

SMAT Overview
The SMAT application enables authorized users to manage access to UW’s Enterprise Data Warehouse (EDW) data in accordance with UW data security policy. Access to EDW data is governed and managed by the Data Management Committee (DMC), whose charge includes assuring security and expanding access to the EDW. SMAT is a web-based front end to the Data Access Control (DAC). DAC is the security database that defines the EDW tables, views, rows and columns that EDW users are allowed to access. Using SMAT, Data Custodians can grant full access to individual EDW tables, or restrict access by role at the column and/or row level, as defined by the DMC’s Roles & Access matrix.

The term ‘SDEF’ is used throughout this document. SDEF stands for ‘Security Definition’, a term given to the security metadata definition assigned to a Role for a given table or view. SMAT provides the functionality to define SDEF and facilitate its promotion to production in the DAC.

SMAT Roles and Responsibilities
Two user roles are authorized to use SMAT: Users and Administrators.
SMAT users (Data Custodians and their designates) are expected to understand the data access business rules within their subject area and are responsible for applying them correctly. SMAT Users are authorized through ASTRA.
SMAT administrators (Enterprise Information, Integration & Analytics business analysts) approve submitted security documents and are responsible for confirming that the SMAT application has been used correctly.

SMAT Tips and Support
- SMAT is located at https://ucs.admin.uw.edu/SMAT
- To request access to SMAT, send an email to help@uw.edu
- Internet Explorer is the recommended browser. Other browsers are not supported.
- For best viewing results, set your monitor to the maximum resolution available.
- Save frequently! Sessions expire after 60 minutes of inactivity.
- For support with the SMAT application, to report technical issues, or for any questions with SMAT, contact help@uw.edu.
- If you would like to provide feedback about the SMAT, please fill out the online survey at https://catalysttools.washington.edu/webq/survey/alchin/68804.
SMAT Process – The Quick Look
This section provides a high level overview of how the Security Metadata Definition (SDEF) is maintained in SMAT.

Apply Security Definition

Figure 1: Apply Security Definition

‘Apply Security Definition’ allows SMAT Users and Administrators to create role-based SDEFs on a new EDW table or view, or edit an existing SDEF on an object.

After making changes to the SDEF, SMAT Users can ‘Save’ or ‘Submit’ changes. ‘Save’ merely writes the changes to the DAC database, while ‘Submit’ initiates an email notification to SMAT Administrators for approval.

After receiving email notification from the User, SMAT Administrators use this form to approve or reject submitted requests. After the SDEF is approved, it is ready for users to test in the test environment.
Submit for Publication

‘Submit for Publication’ serves two purposes: to allow the User to submit a request for an SDEF to be published to production, and allow the Administrator to promote it to production.

After SMAT Users have tested the SDEF, they visit this page to indicate which SDEFs are ready to be moved to production. When the request is submitted, a notification email is sent to the SMAT Administrators.

SMAT Administrators review and submit SDEFs for promotion. The data is put in a queue and the promotion is performed by an automated agent during off hours.
Review Publication Status

The Publication Status page serves as a report where users can check on the status of their promotion requests, and see when the last action was taken and by whom.
Help Page

Figure 4: Help Page

‘Help’ provides an overview of the SMAT application. This page links to SMAT instructions for new and returning users. It also defines the Roles and Responsibilities of SMAT Users and Administrators and provides a support link to the UW-IT Help desk.

Session Timeout
Sessions expire after 60 minutes of inactivity. After 55 minutes, you will see a warning that the session will expire in 5 minutes if no further actions are taken. Edits must be saved before the session expires or they will be lost. Save frequently! Checking boxes within the column and row level selection grids will not renew the session. Menu changes, clicking on buttons like Save and Submit, or typing in a text box will all reset the expiration clock.

SMAT Process - Step-by-Step
This section provides detailed instructions on use of SMAT and security metadata maintenance.
For each of the steps below, start by selecting a task on the navigation bar. The selected page is indicated by the yellow font.

**Step 1: SMAT User changes an SDEF**

1) Select ‘Apply Security Definition’ on SMAT Navigation Bar. (Figure 5) 2) Choose Database and Table Name and click on ‘Load’.

3) Select ‘Change’ to open the form for updates. (Figure 6)
4) Three access levels are available for each table. (Figure 7) Apply the necessary security settings, as needed:

a. Table level
   This is the broadest access level. To grant access to the entire table for all roles, check ‘Unrestricted Table Access’. The Column Name – Role checkboxes will be cleared and unavailable. See [a] in Figure 7.

b. Role level
   This is the next most broad access. To grant or restrict access to the entire table for selected roles, check or uncheck ‘Roles’ on the top yellow row, “Indicate Access to Table For Each Role”. Make sure you have unchecked ‘Unrestricted Table Access’. See [b] in Figure 7.

c. Column level
   To restrict access at the column level, set ‘Restricted Column’ dropdown to ‘True’ and choose roles that should have access. Make sure you have unchecked ‘Unrestricted Table Access’. See [c] in Figure 7.

5) ‘Optional Comments’ is a place to note the history of changes, who made changes, or special considerations for this table. It can also be used for further communication between the SMAT User and Administrator.
6) ‘Save’ or ‘Submit’ your changes:

‘Save’ writes the SDEF to the DAC database but does not trigger any further action. Use this button if you want to save your work but are not ready to promote it.

Use ‘Submit’ to create the DAC view in the testing environment. This action sends email to the SMAT Administrators, requesting that they review and approve the SDEF.

7) To remove your login credentials from the browser session and protect data security, select ‘Logout SMAT’.

**Table Locking:** When you are making changes to a Table, the data is locked for your exclusive use. This prevents others from making changes to the Table security while you have it open. The table lock is released when any of the buttons are activated: Save, Submit, Close or Logout SMAT. If you exit from the browser using the ‘X’ in the upper right corner of the browser, the table lock will remain. To unlock the table, you need to log in to SMAT again, open the Table, and complete the request.

**Time Out:** This form will timeout after 60 minutes of inactivity, so save the form often as you are working on it. If timeout occurs, all unsaved changes will be lost!

**Status** is displayed in the header area following the Database & Table name. In this case, status is ‘changed’.

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Table has no security metadata definition assigned.</td>
</tr>
<tr>
<td>Saved</td>
<td>SDEF has been changed but has not been submitted to the Test environment.</td>
</tr>
<tr>
<td>Processed</td>
<td>The view has been created in the Test environment, but not in Production.</td>
</tr>
<tr>
<td>Submitted</td>
<td>SDEF has been tested and submitted for approval or rejection by the SMAT Administrator.</td>
</tr>
<tr>
<td>Approved</td>
<td>SDEF has been reviewed by SMAT Administrator and is in the queue to be promoted to production.</td>
</tr>
<tr>
<td>Rejected</td>
<td>SDEF was not approved by SMAT Administrator and will remain in Test until resolution.</td>
</tr>
</tbody>
</table>
Step 2: SMAT Administrator approves submitted request.

Figure 9

‘Approve’ and ‘Reject’ options are available only to SMAT Administrators. An ‘Approved’ request will create the DAC View in the testing environment.

1) SMAT Administrator reviews SDEF change requests and will ‘approve’ or ‘reject’ the request. (Figure 9)
2) Email notification is sent to the SMAT User who requested the change and to SMAT Administrators for both approved and rejected requests.
3) An ‘Approved’ request will be submitted immediately. Check on the status of the request in the ‘Publication Status’ report. The delay should be no more than a few minutes.

Step 3: SMAT User tests security metadata

SMAT User must exercise the SDEF in the test environment to ensure it is correct. Here are some guidelines to use for testing:

• Using Reporting Services, go to the DEV or TEST environment. The shared data sources in both environments point to the test databases.
• If a report using the DAC view does not exist, a new one will need to be created.
• Log in using the different roles defined in the SDEF. Run the report and verify security access has been applied correctly and accurately.
• Another alternative is to use SQL Management Studio. Test by logging in as ‘netid’ assigned to a specific role.
Step 4: SMAT User submits security metadata for publication

After SMAT User has tested the SDEF, it is ready to be published. This step notifies the SMAT Administrator to promote it to production.

1) Select ‘Submit for Publication’ on the navigation bar. (Figure 10)  
2) Select search criteria for the security metadata.  
   Hint: Two recommended search options are by the Database and Table, or by ‘Last Published Test Date’ greater than a date prior to the last approval date.  
3) Click on ‘Search’.

4) A filtered list of security definitions is displayed. (Figure 11)  
5) Mark the checkboxes in ‘Request publication to Production *dc’ for each SDEF that is ready for promotion.  
6) Click on “Submit” button.  
7) An email notification is sent to the SMAT Administrators that a request is pending.

Step 5: SMAT Administrator promotes request to production

1) Select ‘Submit for Publication’ on the navigation bar. See Figure 10 in Step 4.  
2) Select search criteria for the SDEF.  
3) Click on ‘Search’.  
4) A filtered list of security definitions is displayed. See Figure 11 in Step 4.
5) To publish to production, check checkboxes in ‘Promote to Production *dss’ for each SDEF.
6) Click on ‘Submit’ button.
7) An automated job is queued which will promote the SDEF to production during off hours.

**Step 6: SMAT Users or Administrator reviews the security metadata published status**

Use ‘Publication Status’ to track the progress of a publication request.

1) Select ‘Publication Status’ on the navigation bar. (Figure 12)
2) Select search criteria. 3) Click on ‘Search’.

4) The Publication Status Page returns a list of SDEFs based on search criteria. (Figure 13)
Step 7: Closing your SMAT Session

1) To log out and exit the SMAT application, click the ‘Logout’ link at the top of the screen (Figure 14) or the ‘Logout SMAT’ button at the bottom of some screens. This will remove your login credentials from the browser and ends your SMAT session but will not save any unsaved work. Be sure to ‘Save’ or ‘Submit’ first!

2) Do not click the ‘X’ in the upper right corner of the browser to close or logout. This will retain the lock on any records that you have selected.