Comprehensive Review of UAccess

Up Next - UAccess Student, Financials, and Research

It has been three years since the last comprehensive review of the UAccess Student, Financials, and Research systems. UAccess roles and user access are required to be reviewed once every 3 years in accordance with the ISO-P702M Procedure. We are in compliance on all system reviews and are preparing for the first of the three reviews this year. First up... UAccess Student!

Here is the timeline for the UAccess Student review.

<table>
<thead>
<tr>
<th>May 14th – May 25th</th>
<th>Kick-off! One-on-one meetings with Data Stewards</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 28th – July 6th</td>
<td>Data Stewards review roles and user access.</td>
</tr>
<tr>
<td>July 9th – July 27th</td>
<td>Data Steward and Business Analyst meetings to go over any questions on role changes that were requested by the Data Stewards.</td>
</tr>
</tbody>
</table>

During the user access review, if the Data Steward is not sure if someone requires a certain role, they will have the option to delegate that review to that user’s Access Provisioning Liaison (APL). EAST will notify the APL if they are delegated any users to review. Not all APLs will have something delegated to review.

EAST will coordinate with the Data Stewards to determine the timeline for the comprehensive review of the Financials and Research system sometime later this year. Stay tune for more details.
New Template Functionality in APT

Available now, a new function in APT called Templates. You can use Templates to create a new request from a request that you have previously submitted. This is especially nice if you want to replicate requests for users with roles based on job duties. Templates only works with requesting access (does not apply to access removal). Please follow the instructions below to create your templates.

1. **Create a Template** - To create a template from a previously submitted request, click the ‘My Requests’ link at the top-right of the page, find the request you'd like to create a template from, and click the "Make Template" button. Note that templates can only be made from requests that have already been submitted.

To view details of all your templates, click on ‘My Templates’. Click on ‘View Details’ to view Basic info and Role Details saved for each template. Click ‘Delete Template’ to remove the template permanently.
2. **Create a New Request using a Template** - To create a new request from a template, click the ‘New Requests’ link at the top-right of the page, enter the name or NetID of the subject, select an Access Provisioning Liaison, choose a Request Type and Request Reason, and type in a Business Justification, and click ‘Continue to role selection’. You have a choice of selecting roles individually under the ‘Select Access/Roles’ or apply a template you previously saved with ‘Select Template’ in your new request. Note, you can compile multiple templates and individual roles in the same request.

3. **Apply Template without Row Level Security** - When you choose to apply a template WITHOUT row level security, all of the Roles that you choose that require you to answer row level security questions will appear just above the ‘Select Template’ section of this page, and in the same location that Roles appear after you select a System and Subject Area. Review the Business Justification field and add more information if needed. Click Submit. You will then need to select each role and answer the row level security questions, and save them. Any roles that do not require row level security will automatically be added to the request.

4. **Apply Template with Row Level Security** - When you choose to apply a template WITH row level security, all of the Roles, including roles with row level security, will be added to your request based on the values you entered on the template. This is appropriate when you need the exact same security settings as someone else in your department whom the template was modelled after. Review the Business Justification field and add more information if needed. Click Submit.

5. **The Business Justification field** is where you can change or add more detailed justification for selected roles, before you click Submit to add the roles from the Template to your request.
Elevated Privilege Training News

Change of Cycle Timing:

Some of you requested we change the cycle periods from June and December so as to accommodate folks who are gone during the Summer and Winter breaks. The cycles run in October and April. This eliminates the unnecessary removal of access during employee absence, since most people are here during those times.

Elevated Privilege Training Is Moving to Learning:

We hope to have the Elevated Privilege (EP) training moved to the UAccess Learning system soon. The full training version has been shortened from 17 minutes to 11 minutes. The first time an existing Elevated Privilege user goes to Learning to renew, they will be **required to go through the entire course**. Afterwards, they will be able to go directly to the attestation portion, just like today. Watch for an email from EAST for more details.

New Systems in the APT

We have installed 2 new systems in the Access Provisioning Tool (APT):

**UAccess Planning**

*UAccess Planning is the system for budgeting, forecasting, and multi-year commitment management.*

**Reserved – College of Medicine**

*The MedLearn Ecosystem is only for use by the College of Medicine.*
Going on Vacation?
How to Delegate Your Approval Tasks

With summer vacations upon us, please take a moment to consider if you will need to delegate your access request/approval tasks to another APL, Dean, or Department Head. A vacation ‘rule’ can be created in the UAccess Access Provisioning Tool by following these instructions:

1. Select Approve and Monitor Requests in the APT https://apt.uaccess-aws2.arizona.edu/
2. Click the link for Preferences.
3. On the Vacation page, set the dates of your vacation and Save.
4. Click Create to begin creating your vacation rule.
5. Give the rule a name.
6. Leave the default checkbox ‘Rule should only apply from [your vacation] dates’ checked, and click Create.
7. Skip to ‘Task the following action:’ and select the Delegate To. Specify your Delegate by NetID. If you do not know your delegate’s NetID, use the flashlight icon to look it up then SAVE.

APL Roles and Responsibilities

Since new APLs are designated on a regular basis, we’ve reserved this space to explain basic Liaison roles and responsibilities. Welcome all new APLs!

Liaison Roles

- Act as a primary contact for the college/business unit for access related work and issues regarding access provisioning/access reviews/changes/removals
- Become the college/department local subject matter expert in access provisioning
- Understand, communicate and drive security concerns as they relate to the end user and the access they have

Liaison Responsibilities

- Act as the primary contact for receiving, reviewing, distributing and collecting necessary information relating to access
- Participate in the work flow overseeing/approving/requesting access or access removals
- Monitor department user training needs as they relate to access provisioning
- Monitor and insure that department users who have elevated privileges complete required annual training
- Review and distribute access provisioning communications to appropriate personnel