Access Provisioning Liaison Newsletter

Elevated Privilege Training – First Round an Astounding Success!

With your help and attention to detail, we recently completed the first training period for Elevated Privileges. We are pleased to announce Review Period One has concluded with very positive results!

- 3,795 individual users were contacted about the need to complete training
- 183 APLs received worksheets of users in their departments who needed to complete training
- 168 individual users had roles removed during the process because upon review the roles were determined to be unnecessary for the users job duties
- 3,690 individual users completed the training on time!
- 14 individual users had roles removed due to a lack of training compliance
- 29 users were believed to be inactive, which upon further review 4 users appear to be truly inactive
- ~ 30 users were dropped due to operational issues with the tool developed to manage the process. These users will be picked up in the next Training Review Period.

Remember, Elevated Privilege Training has been added as a prerequisite to obtaining access to the UAccess Employee and Student Systems, but UAccess Financials and Research require periodic review due to the nature of dynamically assigned roles. Additional systems will be added to the training in the future (e.g., Analytics High Access).

Elevated Privilege Training – continue to Page 5.
Audit Concern: Terminations Not Always Submitted In A Timely Manner

Did you know that EAST plays a supporting role in the Financial and IT Audits that the University completes every year? EAST provides information and data related to the access granted and managed for users of the UAccess Enterprise Applications. Auditors request data in order to ‘test’ the processes and procedures used to grant new access and remove old access to the UAccess Systems.

In the latest Financial Audit, an area of concern was related to the removal of access for terminated employees. A significant number of terminations were identified with large gaps between the date of separation and the date Manager Self Service transactions were submitted by initiating departments. Although EAST removes access weekly for users reported by Systems Control as having terminated, deceased, or retired within the last 7 days—Systems Control is reliant on departments promptly submitting Manager Self Service (MSS) termination transactions.

4 reasons terminations need to be submitted in a timely matter:
1. Timely removal of access to University Systems
2. Timely review and removal of access to University Physical Assets and Buildings
3. Timely Payroll and necessary payouts
4. Adhere to State Law for involuntary terminations

To help prevent future audit findings, please review your departmental practices for processing termination paperwork and any related departmental guidelines.

New Roles Available in UAccess Access Provisioning Tool (APT)

The following new roles have been recently added to APT.

UAccess Student
PERC Roster Update refers to Post Enrollment Requirement Check. This role grants access to run a roster that captures and stores the status of a student’s enrollment requirement for that class. Intended for department/college users are responsible for enrolling students in courses for their department.
UAccess Student – Campus Users > Student Records > PERC Roster Update.

An Online Training Course is a prerequisite to gaining access to this role; see the UITS Workshops page.

Grad Coordinator provides access to approve/deny GradPath forms as well as the ability to run the Master’s Completion process.
UAccess Student – Campus Users > Graduate College > Grad Coordinator.

New Analytics Dashboard for Understanding My UAccess Roles

Through collaboration between the UITS Training Team, Enterprise Information & Analytics, and EAST, a new dashboard called My UAccess Roles and APL has been made available to campus users from the Analytics home page. No Analytics security roles are required in order to access this page.

This dashboard is intended to provide Users a means to review their own UAccess security roles and related provisioning information. It displays one’s own Access Provisioning Liaison(s), Completed Prerequisites (i.e. FERPA, UAccess User Attestation, Elevated Privilege Agreement) and UAccess system roles.

Find the My UAccess Roles and APL dashboard at the UAccess Analytics home page, on the bottom-left under the Get Started heading.

On a related topic, does your department know YOU are their APL? Do the staff who commonly request access know you are the person to whom UAccess system requests should be routed for approval? If you have not already shared your very important APL role with staff in your department – please consider doing so! Tell them you can assist with

- Identifying access needs and how to request access
- Prerequisites and Training requirements
- Terminations – ensuring access is removed in a timely manner
- Collaborating with EAST!
Help! “Suzie” Just Left and We’re Not Sure What Access Her Replacement Needs!

Has this happened to your department? More importantly, could it?

While we recognize no amount of planning can fully prepare you for the unexpected departure of key staff, there may be some simple ways to document the types of tasks staff in your department handle that require access to UAccess systems. Why should you take proactive steps to document tasks and required access? Well, do you know which staff handle the following tasks?

- Pay requests? Department funding changes?
- Financial aid awards and stipends?
- Add courses to the schedule of classes or to the curriculum?
- Do you know how to request access for any of the above?

If you could not easily answer these questions, taking an hour or two today may save you several hours in the event you need to backfill key staff.

A simple way to start is by using UAccess Analytics> Stats> Security> All Roles, to look up and then print or export UAccess Role information for your key staff members. Although the technical role name is displayed, it is a very good basis for using other available documentation and tools published by EAST to obtain additional information.

Once the tasks performed per staff are understood and you know the UAccess Roles the person has, you have a basis to understand how to request the corresponding roles in the UAccess Access Provisioning Tool. For many, this is where things become difficult. Take baby steps. Document the ones you know, or ones you have frequently had to request for staff in your area. When you get stuck, contact us! We’re happy to help.

Q and A with EAST

APL Question: Regarding Elevated Privileges Training, there are a number of users in my area who do not work on the main Tucson campus. Many of them had trouble accessing the Agreement at the end. Is that going to be fixed next time?

EAST Answer: Yes, for the next training review period, it will no longer be necessary to connect to the main campus network using VPN in order to access the Elevated Training video, nor the Agreement at the end.

APL Question: I had staff who were on sabbatical or LOA for whom I requested a waiver from training for the first Elevated Privilege training period. For how long are the waivers valid?

EAST Answer: The EP waivers from training are only valid for the current training period. These users will be notified of the training requirement again with the next training period, and will be included on APL reports. If needed, new waivers will need to be requested by contacting EAST.
Going On Holiday?

**How to delegate your approval tasks**

With the holidays and Winter Closure upon us, please take a moment to consider if you will need to delegate your access request/approval tasks to someone else. A vacation ‘rule’ can be created in the UAccess Access Provisioning Tool by following these instructions:

1) Access the **UAccess Access Provisioning Tool**, and click **Approve and Monitor Requests**.
2) From the Approval dashboards, on the far upper right, 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; this can be whatever is meaningful for you.
6) Leave the default checkbox ‘**Rule should only apply from [your vacation dates]**’ checked, and click **Create**.
7) Do not add a Condition. Instead, skip down to ‘**Task the following action:**’ and select the **Delegate to** option.
8) Specify your **Delegate** by NetID. If you do not know your Delegate’s NetID, use the flashlight icon to look it up.
9) **Save** your updates.

If possible, we recommend setting up your vacation rule a day or two **prior to leaving the office**, so you can verify with your Delegate that it is working as you both expect. Keep in mind you will continue to be notified of and have the ability to approve requests routed to you during the dates you have set for your vacation rule.

**APL Roles and Responsibilities**

Because new APLs are delegated on a continuing basis, this space will be reserved for Liaison Roles and Responsibilities.

**Liaison Roles**

- Act as a Primary Contact for the college/business unit for Access related work and issues with regard to Access Provisioning/Access Reviews/Changes/Removals/Related Activity
- Become the college/department local subject matter expert in the area of Access Provisioning
- Understand, communicate and champion security concerns as they relate to the end user and the access they have been privileged to receive

**Liaison Responsibilities**

- Act as the Primary Contact for receiving, reviewing, distributing and collecting necessary information relating to access
- Participate in the work flow for overseeing/approving/requesting access or access removals
- Monitor Department User training needs as they relate to Access Provisioning
- Monitor and insure department users who have elevated privileges complete necessary annual security training and acknowledgements and/or agreements
- Review and disseminate Access Provisioning Communications to appropriate college/department personnel and users

**Did You Know?**

Did you know that during the UAccess system implementations (2+ years ago), system access was ‘grandfathered’ in for Users who **had not completed the UAccess User Attestation and/or the FERPA tutorial**? While we intend to notify these Users and their APLs of this non-compliance issue soon, we kindly suggest that you check for such Users in your area **now**, and direct them to complete these prerequisites at their earliest convenience.

To do so, use the **Analytics > Stats > Security > Prereqs** dashboard and look for Users in your area by filtering for the following combos:

- SA Access = Yes and FERPA = No
- SA Access = Yes and Attestation = No
- HCM Access = Yes and Attestation = No
- BI Access = Yes and Attestation = No

Keep in mind only Users with **more than self-service access** are required to complete these prerequisites.
Elevated Privileges – Success!

While this is an annual training for individual users, after a brief lull for operational improvements, EAST will manage this process quarterly to insure coverage/compliance. This means we will be in communication with you regarding new Elevated Privilege users throughout the year. We anticipate the second review period will begin in January.

Thank you for your part in this tremendous success story. We have shared this success story and your part in it, with UITS Leadership, the ISO, the CIO and our Data Stewards and Authorizing Agents. Thank you and Kindest Regards from EAST!

Detail Stats:

<table>
<thead>
<tr>
<th>Communications</th>
<th>Date</th>
<th>APLs</th>
<th>Users</th>
<th>Training Verified as Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle 1</td>
<td>9/4/2012</td>
<td>183</td>
<td>3795</td>
<td>44</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>9/27/2012</td>
<td>176</td>
<td>2001</td>
<td>1760</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>10/25/2012</td>
<td>137</td>
<td>627</td>
<td>1317</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>11/2/2012</td>
<td>87</td>
<td>141</td>
<td>465</td>
</tr>
<tr>
<td>4.1</td>
<td>11/5/2012</td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>4.2</td>
<td>11/7/2012</td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>4.3</td>
<td>11/9/2012</td>
<td></td>
<td></td>
<td>57</td>
</tr>
<tr>
<td>Proactive phone calls for APLs w 4 or more non-compliant Users</td>
<td></td>
<td></td>
<td></td>
<td>18</td>
</tr>
<tr>
<td>4.4</td>
<td>11/26/2012</td>
<td></td>
<td></td>
<td>34</td>
</tr>
<tr>
<td>Total Trained via This Review Process</td>
<td></td>
<td></td>
<td></td>
<td>3690</td>
</tr>
</tbody>
</table>

Community Response

<table>
<thead>
<tr>
<th>APL Inquiries</th>
<th>Cycle I</th>
<th>Cycle II</th>
<th>Cycle III</th>
<th>Cycle IV</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>APL Complaints</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Customer Inquiries</td>
<td>53</td>
<td>102</td>
<td>66</td>
<td>25</td>
<td>246</td>
</tr>
<tr>
<td>Customer Complaints</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Technical Problems</td>
<td>71</td>
<td>47</td>
<td>39</td>
<td>5</td>
<td>162</td>
</tr>
</tbody>
</table>