2nd Assignment Stats and Next Assignment

Thank you to the many of you who completed the 2nd Assignment: the review of UAccess Student access. 1336 Users/Roles were removed per your requests, and countless questions answered! If you have not yet completed your assignment, or have lingering questions, please contact us.

The next assignment will be a Department/Title Change review to be distributed by early August. In order to keep the amount of data requiring your review to a minimum, we intend to ask for this review on a quarterly basis. Department/Title Change data will be extracted from UAccess Analytics going back to mid-February 2011, or the point by which we pulled this data for the first assignment. However, if you did not return the first Dept/Title Change assignment, you will be asked to review those same staff/their access with the next Dept/Title Change review, as well as any new department/title change data.

Future access review assignments are planned to include:

- A one-time notification to APLs of UAccess system users who have not completed FERPA training and/or the Acceptable Use Policy.
- Implementation of yearly training for users with elevated privileges and/or access to sensitive data

UAccess Student and UAccess Employee Upgrade is a success!

UAccess Student and UAccess Employee systems were upgraded as of July 18. See http://mosaic.arizona.edu/upgrades/benefits for additional information.
Upcoming APT Enhancements

Important enhancements to the Access Provisioning Tool (APT) are nearing completion!

- A new option to request Access Removals will be available in July 2011. The Access Removal system will be flexible, providing options for requesting Access Removal for employees who have terminated, as well as removal of specific system/role(s) for employees whose job duties no longer require the access. The Access Removal system will be discreet; no notification will be sent to the employee. Watch for a release announcement later this month!

- UAccess Student Roles will be available for request via the APT later this summer. Because requests for access to UAccess Student are currently handled by email; the addition of UAccess Student Roles to the APT will remove manual processes, provide complete records of approvals, and improve the accuracy and timeliness of UAccess Student provisioning.

Similar to existing request processes for other UAccess systems, UAccess Student requests will require:

1. FERPA training
2. User agreement to the UAccess Acceptable Use Policy
3. APL approval
4. Data Steward or Authorizing Agent approval per Role/Access Level requested.
5. User Training per Role/Access Level where required.

In addition, documentation and tools are being prepared to assist you in determining what access to request for your staff in the enhanced APT. Watch for further updates to the APL listserv.

Sponsored Collaborators Project

Some of you may have heard of the UAccess Employee system enhancements being planned with regard to Sponsored Collaborators, or POIs, DSVs, and other Affiliate types. In addition to providing a more streamlined process for managing Sponsored Collaborators in your department or college, the new enhancements will have a positive effect on existing access provisioning processes as well. For example, improved options for managing end dates will allow EAST the ability to create accurate termination reports for de-provisioning. Also for terminations, a “disable security access on XX date” option will provide business managers the ability to specify whether or not systems security should be removed, and when. Finally, the list of Collaborator types allowed UAccess systems access will be revised. The implementation of the Sponsored Collaborators systems enhancements is currently slated for Fall 2011.

Looking for Volunteers

EAST needs to identify a group of APLs who would like to participate in the Requirements Definition for a comprehensive Access Management tool. The primary objective will be to gather requirements and evaluate commercial off-the-shelf solutions in order to identify the long term strategy for enterprise access management. Requirements will cover access requests, removals, access reviews and monitoring, training, and more. If you would like to have a voice and participate in this process, please contact EAST. We will begin this requirements gathering effort in September 2011.
APL Resources

For the many new APLs delegated since the orientation sessions held in March 2011, please take note of the following resources:

- APL Orientation Materials posted on our SharePoint site under “Documentation.”
  [https://sp.mosaic.arizona.edu/SiteDirectory/AccessProvisioningLiaisons/default.aspx](https://sp.mosaic.arizona.edu/SiteDirectory/AccessProvisioningLiaisons/default.aspx)

- UAccess Analytics Security dashboards – available to users who have HR-Medium access. Users can confirm what level(s) of Analytics access they have on the main Analytics page, in the grid labeled “My Roles.” The Security dashboards are located under Stats > Security, and include the following:
  - All Roles dashboard - provides the ability to look up UAccess user roles by NetID, Home Department, DeptId, or Last Name
  - Approval Authority dashboard - provides the ability to look up APL delegations by NetID, Home Department, or Authorized Departments. *Note: this is the tool Data Stewards use in reviewing access requests to confirm the correct APL authorized the request for the department/college.*

- UITS Training Workshops site for information on free training for UAccess systems. Includes links to available workshops list, training guides, and instructions for registering for a session.
  [http://uits.arizona.edu/workshops/current_workshops](http://uits.arizona.edu/workshops/current_workshops)

Q and A with EAST

APL Question: “On a recent assignment, I noticed some student employees for my department were not listed. They have UAccess systems access for their job. Why wouldn’t they be listed on my assignment?”

EAST Answer: This likely has to do with employees with multiple jobs and the means by which we match Users to APLs. Up until this point, we matched Users to APL using the Home Department as it appears in Analytics, without taking extra steps for Users (whether students or employees) with multiple jobs. This has meant such Users only appeared on the assignment of the APL for one of their jobs, when they should appear on the assignments for APLs of departments matching all of their jobs. This oversight has uncovered another issue: some APLs have requested removal of access for Users with multiple jobs for whom they were not aware was authorized for the access through another job/department. To remedy this in the future, EAST will take extra steps to match Users with multiple jobs to all relevant APLs.
Annual Review

Access Provisioning is an important task for which EAST has played an integral role in support of the Mosaic Project. UAccess Employee and UAccess Student Users have been provisioned either in mass as part of key system implementations, or through daily operational processes managed by EAST.

The continuing nature of software development, such as the phased Manager Self Service implementations, requires the iterative provisioning of access. This development is expected to continue throughout the 11/12 fiscal year. EAST will continue to support these and similar releases of new functionality, including the UAccess Financials system implementation taking place in Fall 2011, on an ongoing basis.

FYE 2010/2011 Statistics:

**UAccess Employee**
Users/Roles Provisioned = 27,904

**UAccess Student**
Users/Roles Provisioned = 14,623

SharePoint Woes

Are you one of the APLs who continues to have trouble accessing the APL SharePoint site? We want to hear from you! While our desktop support staff was able to contact several of you to resolve the issue, we want to reach out to those who may not have reported the issue previously. To access the site, keep in mind the following:

- You must be connected to the main campus network OR the University of Arizona VPN.
- Use Internet Explorer.
- Sign-in using your NetID and password. Many users have had to prepend their NetID with the word CATNET as follows: **CATNET\NetID** (where ‘NetID’ is replaced with your NetID)
- If problems persist, please contact us at 621-4214 for troubleshooting. Be prepared to describe any error message or ‘what happens’ in detail.