Enterprise Applications Access Review

Scope

These procedures summarize how administrative access to UAccess and other enterprise applications are approved and managed at the University. Topics include:

- Stakeholders
- Tools
- Access Authorization
- Review of Access
- Terminations
- Department Transfers

Stakeholders

Requestor - A person who submits a request for administrative access to UAccess and other enterprise applications for themselves or another.

Recipient (User) – A person who needs administrative access to UAccess and other enterprise applications.

Access Provisioning Liaison (APL) – A person who reviews/approves requests for granting, modifying, or removing administrative access based on business needs.

Data Steward (Information Owner*) or Delegate – A designated University representative who owns and manages institutional data and who has the responsibility of ensuring that the appropriate steps are taken to mitigate risk.

Business Analyst (BA) – A person who works with the Data Steward or Delegate to identify needs and gather requirements for changes to security roles. They also provide additional information as needed when access is requested.

Security Administrator – An Enterprise Applications Security Team (EAST) member or other designated person responsible for the creation, deletion, and maintenance of user access.

* See https://policy.arizona.edu/information-technology/identity-and-access-management-policy
Tools

**Access Provisioning Tool (APT)** – The primary application used to request access to UAccess and other enterprise applications.

**Access Approval Workflow (AAW)** – The primary application used to approve and house APT requests.

---

Access Authorization

A recipient’s department will determine when administrative access is needed to UAccess and other enterprise applications based on legitimate business need, and will request the access via the APT. The recipient’s department is responsible for ensuring the recipient completes applicable prerequisites and attends any training required. The APL will review the details of the request and approve or deny the request before the request proceeds to the next reviewer in the AAW.

If applicable, the Business Analyst will review the details of the request and provide additional information as needed.

The Data Steward or delegate will review the details of the request, ensuring that the role requested is appropriate for the recipient based on the business needs and justification provided. They will approve or deny access before the request proceeds to the next reviewer in the AAW.

After all workflow approvals have been completed, the Security Administrator will verify completion of required training before provisioning the approved request and will notify the recipient and requestor that access has been granted.

---

Review of Access

Access to UAccess and other enterprise applications will be reviewed periodically in accordance with the following procedures.

1. **User Review**
   a. The APL will review users who have transferred departments or changed positions within their department for continued appropriateness of access.
   b. The APL will annually certify review completion and take appropriate action if needed.

2. **Role Review**
   a. The Data Steward will review security roles that they own or manage that have been modified since the last review. The Data Steward ensures that the scope of access is appropriate for each role.
b. The Data Steward will certify their review completion and take appropriate action if needed, by working with their Business Analyst.

3. **Security Change Control**
   a. The Business Analysts will notify the Security Administrator of any changes to security roles.
   b. Prior to security changes moving to production, the Data Steward will review and approve, ensuring that the scope of access is appropriate.

---

**Terminations**

When a user leaves the University, their administrative access will be revoked.

The APL or user’s department is responsible for submitting an access removal request through the APT no later than 5 business days after the recipient’s last day at the University.

The Security Administrator will process removal requests that were submitted by the department through the APT.

---

**Department Transfers**

When a user leaves a position, their administrative access will be revoked unless justified as defined below.

The APL or user’s former department is responsible for submitting a removal request through the APT no later than 5 business days after the recipient has transferred departments.

The APL or user’s new department is responsible for submitting a request through the APT for any needed administrative access.

If the user’s administrative access, all or in part, needs to be retained by the new department, a detailed request needs to be submitted through the APT prior to the recipient’s last day in the former department to avoid any loss of access.

The Security Administrator will remove all administrative access not requested by the new department.

---

**Revision History**

| Final draft | 04/22/2020 |