UAccess Application Access Provisioning
At-A-Glance Quick Reference Guide

Understanding The Data Steward and Authorizing Agent Responsibilities

Data Stewards are defined as the persons who are ultimately responsible for the integrity and safety of the Institutions data at an executive level. Data Stewards may delegate their oversight responsibilities to an Authorizing Agent in order to facilitate the day to day operation of the Institution’s business.

Data Stewards and Authorizing Agents authorize or control access to the primary transactional business systems of the University and thereby authorize or control access to University data. The primary transactional business systems are generally referred to as “Enterprise Applications.” The UAccess Systems are Enterprise Applications. Authorized Agents are established for each UAccess System Subject Area, in accordance with the Access Control Standard for the authorization, modification, review, and revocation of a user’s access, as well as the University’s Data Access Policy.

For the purpose of this document a Data Steward or Authorizing Agent is defined as a person responsible for validating Access Requests, and approving and granting said access.

References:
University of Arizona Data Access Policy
Information Security Office
Procedure Title: Enterprise Applications Account Access
Procedure Number: IS-P701
Responsible Office: Office of Information Security

Access Requests

If you are a Data Steward or an Authorized Agent of a Data Steward, you may receive Requests for Access to UAccess Systems. Your role in the request approval process is to:

- Review the Request for Access, including giving critical consideration to:
  - The Department Approver – the Department Approver must be an authorized Access Provisioning Liaison (APL). Each Department and College has one or more authorized APLs. These persons are the only persons for the Department / College who may approve Access Requests for users in their area. An APL may submit ‘and’ approve such a request. Or, the APL may approve a request submitted by an employee supervisor or even an employee requesting access for them self. The key is that a person may not approve their own Access Request; meaning the employee who needs access may not be the approver; an APL may not approve a request for their own access. The Access Provisioning Tool will preclude a person from approving their own access.
  - The Employee Needing Access – the Employee’s department and job title information is included in the Request for Access. Critical consideration should be given to whether or not the employee’s information makes logical sense in correlation to the access being
requested. A Requestor or Access Provisioning Liaison may include additional information or add comments to a request, to help approvers understand the specific job needs and business justification for the request. As the Data Steward or Authorized Agent, if you are not comfortable with the access request, you can

- **Request additional information** – from one of the persons involved in the workflow up to the point it reached you. If you request additional information, be sure to remind the person you are interacting with, to send you the ticket after they have added their comments.

- **Delegate the request** – you may send the request to another responsible Data Steward or Authorized Agent, who may have more information or insight to the employee’s needs. In this case you are ‘delegating’ your approval. Once you delegate to another person, you will not receive the ticket back. It will move forward in the approval workflow.

- **Deny the request** – if you are not comfortable with the request you may deny the request by selecting the ‘deny’ Action, available in the approval process.

  - **The Roles being requested** – the roles should make business sense and not cause a segregation of duties concern. Roles which have been identified to have a conflicting role counterpart are identified in the Role Descriptions Document. When in doubt you should request additional information, clarify and/or check available reference documents for Segregation of Duties issues.

  - **Row Level Security requested** – the row level security requested should be included when required and appropriate and applicable for the employee user’s department / job. Roles which require Row Level Security are identified in the Role Descriptions Document. When in doubt you should request additional information, clarify and/or check available reference documents for Row Level Security requirements.

Tools are available to help with the Access Request Review.

- **UAccess Analytics Dashboards** – Data Stewards and Authorized Agents should have access to the UAccess Analytics>Stats>Security dashboards. Analytics HR Medium access is required to see these dashboards. These dashboards include many useful views of Employee, Access Provisioning Liaison and Role / Security data. Of particular interest are:

  - **All Roles** – allows review of all roles and some row level security currently assigned to a specified employee/user.

  - **Approval Authority** – allows review of all Access Provisioning Liaisons (present and past). Selection is available to select an APL by their home department, or to select a Department for which the return result will include a list of APL(s) for that department.

  - **POI / DSV Affiliates** – this dashboard includes a few data views. In addition to including the POI and DSV data, it includes a view of ‘all’ employees regardless of their current affiliation status. Terminated, retired, deceased persons, etc. are included in the all employee view.

  - **HCM / SA Audit** – this dashboard also includes a few data views, including a view of ‘inactive’ employees who may still have non-self service roles for HCM and SA. This list should never be very long, and should only include persons who have changed their affiliation with the University within the last calendar week. It also includes views of FRS users, users with Department or Title Changes.
• **Role Descriptions** – a comprehensive document is available which includes detail role description attributes, including segregation of duty indicators, elevated privilege indicators, row level security and training requirements, the campus community the role typically applies to, how the role is typically requested and who typically provisions the role, and more.

• **At a Glance Quick References** – many short documents are available, addressing various topics related to Access Provisioning.

• A **User’s Guide** is available for the Access Provisioning Tool. This document includes useful information on how to request access, how to approve an access request, how to retrieve, look-up and monitor requests, how to set-up out of office vacation delegation rules, and more. The User’s Guide is available at the following location:

### Role Changes

Roles and Role Permissions periodically change to reflect new business needs, functional or operational discoveries. When a Role or a Role’s permissions change, individuals who have already been approved for the Role may gain greater access than was previously approved. The ISO 701 M Procedures indicate that when a Role or its Permissions change, the Data Steward or Authorized Agents must:

- Approve of the changes
- Participate in the review of users previously granted the subject role

EAST will facilitate the process by communicating with Data Stewards and Authorized Agents when such a change is moving through the production change control process. EAST will also facilitate the user review by providing lists of users and their relevant department and title information. EAST will then retain approved documentation for reference and audit discovery purposes.

### New Roles

Similar to Role Changes, periodically new roles are required to be created. Data Stewards and Authorized Agents must be aware of new roles, and the access that those roles provide users. Often when new roles are created, a list of initial users to receive the new role is also created. This list of users must be approved by the Access Provisioning Liaison as well as the applicable Data Steward / Authorized Agent, prior to access being granted in production. In these cases the access is typically set-up as part of the migration to production, if the number of users is large and warrants this approach.
Access Provisioning Oversight

Although access request are managed and provisioned through the UITS Enterprise Applications Security Team, Data Stewards and Authorized Agents are welcome and encouraged to become very familiar with the EAST Access Provisioning Liaison program, as well as ask questions and understand the processes EAST uses to manage the provisioning and periodic reviews required by the ISO 701 M procedure. EAST anticipates meeting with Data Stewards and Authorized Agents at least once per year to review processes and any operational concerns encountered since the last such meeting.

Additional Assistance

When you need additional information or assistance with any Request, do not hesitate to contact EAST for assistance. A primary responsibility of EAST is to support our Data Stewards and Authorized Agents.