Understanding Data Steward and Authorizing Agent Responsibilities

Data Stewards are ultimately responsible for the integrity and safety of the institution’s data at an executive level. Data Stewards may delegate their responsibilities to an Authorizing Agent in order to facilitate day-to-day business operations.

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, and UAccess Systems fall into this category. Authorized Agents are established for each UAccess System Subject Area in accordance with IS-P702M, Enterprise Applications Account Access (UAccess).

For the purpose of this document, a Data Steward or Authorizing Agent is defined as a person responsible for validating and either approving or disapproving access requests.

Access Requests

As a Data Steward or Authorized Agent of a Data Steward, you may receive access requests for UAccess Systems. Your role in the request process is to review the request, giving critical consideration to:

1. **The Department Approver** – must be an authorized Access Provisioning Liaison (APL). Each department/college has one or more APLs. These 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, they may approve a request submitted by a user requesting access for themselves. The key is that a user may not approve their own access request. Likewise, an APL may not approve a request for their own access. The UAccess Access Provisioning Tool will preclude a person from approving their own access.

2. **The user needing access** – the user’s department and job title information is included in the access request. Critical consideration should be given to whether or not the user’s information makes logical sense in correlation to the access being requested. Requestors and APLs are encouraged to include additional information or 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 take one of the following actions:
   i. **Request additional information** – from one of the persons involved in the workflow before 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.
   ii. **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.
   iii. **Deny the request** – if you are not comfortable with the request you may deny it.

3. **The roles 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 applicable role descriptions document. When in doubt, you should request additional information, clarify and/or check available reference documents for segregation of duties concerns.
4. **Row Level Security requested** – the row level security requested should be included when required for the user’s department / job. Roles which require Row Level Security are identified in the applicable role descriptions document. When in doubt, you should request additional information, clarify and/or check available reference documents for Row Level Security requirements.

The following resources are available to assist with reviewing and validating access requests:

1. **UAccess Analytics Security > Security Dashboard** (requires Analytics HR Medium access) – includes many useful views of Employee, APL and Role/Security data. Tabs of particular interest are:
   i. **All Roles** – shows all roles and some row level security currently assigned to a specified user.
   ii. **Access Provisioning Liaisons** – allows lookup/review of all APLs (present and past). Allows selection based on various criteria including the APL’s authorized departments, Net ID, college code, home department, and name.
   iii. **DCC Affiliates** – in addition to including DCC data, it includes links to view ‘all’ employees regardless of their current affiliation status. Terminated, retired, deceased persons, etc. are included in the all employee view.

2. **Role Descriptions** – comprehensive documents are available which include detailed role description attributes including: segregation of duty indicators, elevated privilege indicators, row level security and training requirements, the campus community a role typically applies to, how a role is typically requested, who typically provisions a role, and more.

3. **Support, How-Tos & Info** - references addressing various topics related to Access Provisioning.

**Role Changes**

Roles and role permissions periodically change to reflect new business needs, functional or operational discoveries. When a role or role permissions is changed, individuals who have already been approved for the role may gain greater access than was previously approved. ISP-702M 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 APL 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 requests are managed and provisioned through EAST, Data Stewards and Authorized Agents are encouraged to become familiar with the APL program, as well as ask questions and understand the processes EAST uses to fulfill the requirements of IS-P702M.