## UAccess Enterprise Applications Account Access Roles and Responsibilities

| UAccess Access Role | Responsibility Area | Responsibility |
|---|---|---|
| **Subject** – Employee needing system access. | | • Ensure access is revoked when terminated, transferred or promoted. |
| **Requestor** – Employee's supervisor who will request system access on behalf of the subject employee. | • **Initial Authorization or Modification of Access** | • Request appropriate access or modification based on legitimate business need<br>• Ensure that the User will attend any training available for the UAccess Enterprise Application(s) as related to the User's job function and the access level requested<br>• Notify authorizing agent when user is transferred, promoted, or terminated |
| **Access Initiator** – First approver in the process, typically a Dean or Department Head. The Access Initiator must be an authorized signer for the department, or another specifically designated person. | • **Initial Authorization or Modification of Access** | • Validate the request, approve or deny the request, and submit approved requests to the Authorizing Agent |
| **Authorized Agent** – The second approver in the process. This can be a Data Steward or person designated by the Data Steward, responsible for validating requests and approving the granting of access. | • **Initial Authorization or Modification of Access** | • Verify the Subject User's active status in UAccess Employee and the authority of the Access Initiator<br>• Direct requests for exceptions to standardized access to the Data Steward<br>• Approve or deny access after receiving and validating the rationale and all approvals |
| | • **Review of Access** | • Determine users to be removed for inactive accounts every 180 days, working with account activator to request removal of access.<br>• Conduct annual sample of the active User base and survey the Users' Supervisors or Access Initiators to determine whether access remains appropriate for a legitimate business need; leave access unchanged, modify or terminate a User's access and make an appropriate log entry to note the review of the User, including the date and the action taken. Notify the Account Activator of any access changes.<br>• Whenever a defined Role and the Role's Permissions are modified, under direction of Data Steward, review its scope of access and distribution across provisioned Users. Notify the Account Activator and the Users, if the review produces changes in the scope or distribution of the Role.<br>• Every three years, under the direction of the Data Steward, conduct a comprehensive review of all defined Roles that have not been otherwise subject to modification during the previous three-year period. Notify the applicable Account Activators and Users, if the review produces changes in the scope or distribution of the Role. |

| | | |
|---|---|---|
| | • **Revocation of Access** | • Quarterly, request a report extracted from UAccess Employee indicating Users who have changed positions within the University. Check reported User's current access level to determine if access is still valid. Note modification and/or removal and return notification of changes to the Account Activator prior to the next scheduled report.<br>• Obtain initial and ongoing training on the procedures for authorizing, modifying, deactivating and reviewing access. |
| **Account Activator** – The third and final approver in the process. The Account Activator represents the individual(s) responsible for actual setup and provisioning of the request. | • **Initial Authorization or Modification of Access** | • Upon approval of Authorizing Agent, set up the approved access and notify the User, the User's Supervisor or the Authorizing Agent that access has been granted. |
| | • **Review of Access** | • Distribute report every 180 days to Authorizing Agent to review for account inactivity. Remove access for users as noted by Authorized Agent.<br>• Modify or remove access as directed by authorizing agent during annual sample for continued appropriateness of use.<br>• Modify or remove access as directed by authorizing agent when defined role or role's permission is modified or during three year cycle of review if review produces changes in scope or distribution or role. |
| | • **Revocation of Access** | • Every two weeks, using a report from UAccess Employee indicating Users who are no longer employees or affiliated with the University. immediately remove access which is no longer appropriate<br>• Remove inappropriate access upon notification by Authorizing Agent for terminations requiring immediate attention.<br>• The Enterprise Applications Security Team will retain report records of modified and deactivated access.<br>• Obtain initial and ongoing training on the procedures for authorizing, modifying, deactivating and reviewing access. |
| **Data Steward -** A person identified pursuant to the University Employee Access to Institutional Data Policy to manage the data of an Enterprise Application | • **Initial Authorization or Modification of Access** | • The Authorizing Agent will direct requests for exceptions to standardized access to the Data Steward, who notify the Authorizing Agent in writing of his/her decision. |
| | • **Revocation of Access** | • Obtain initial and ongoing training on the procedures for authorizing, modifying, deactivating and reviewing access. |