Scope
These procedures apply to individuals authorizing or controlling access to the University’s
- Primary enterprise business systems
  - UAccess Analytics
  - UAccess Employee
  - UAccess Financials
  - UAccess Research
  - UAccess Student
- Direct database table access to all of the above

The applications referenced above are collectively referred to in these procedures as “UAccess Enterprise Applications.” This document establishes procedures in accordance with the Access Control Standard for the authorization, modification, review, and revocation of a user’s access to UAccess Enterprise Applications. It also mandates training of those involved in the access control process.

Definitions
ACCESS REQUESTOR - A person requesting authorization or a person who submits a request for another, for access to UAccess Enterprise Applications.

SUBJECT USER – A person requesting authorization or who needs authorization to access a UAccess Enterprise Application.

DEPARTMENT APPROVER – A person who requests, or reviews requests, for access to UAccess Enterprise Applications and who authorizes the granting, modification or removal of access based on business needs, established policies and procedures. This may only be an Access Provisioning Liaison, Dean, Director, or Department Chair.

AUTHORIZING AGENT – A Data Steward or their delegate responsible for validating requests and approving the granting of access. The Authorizing Agent represents the interests of the University in terms of system and data protection.

SECURITY ADMINISTRATOR – An Enterprise Applications Security Team member or other designated person responsible for the creation, deletion and maintenance of User access.

DATA STEWARD – A designated University representatives who is tasked with managing institutional data owned by the university. The data steward has the responsibility of ensuring that the appropriate steps are taken to protect the data and that respective policies and guidelines are being properly implemented.

UACCESS ACCESS PROVISIONING TOOL – The primary application used to request and record approvals for access to UAccess Enterprise Applications.

Access Authorization
A Subject User’s department will determine when a Subject User needs access to a UAccess Enterprise Application based on legitimate business need and using the UAccess Access Provisioning Tool, and will
relay the request for access to the Department Approver. The Subject User’s department is responsible for ensuring the User will complete applicable prerequisites and attend any training required for the UAccess Enterprise Application(s) as related to the User’s job function and the access level requested.

The Department Approver will review the details of the request, approve or deny the request, and submit approved requests to the Authorizing Agent.

The Authorizing Agent will verify the Subject User’s active status in UAccess Employee and the authority of the Department Approver (typically, by use of the UAccess Analytics APL Dashboard, by appropriateness of job title, use of the eSignature database, or other proxy validation system). The Authorizing Agent will direct requests for exceptions to standardized access to the Data Steward. The Data Steward will notify the Authorizing Agent in writing of his/her decision. The Authorizing Agent will approve or deny access after receiving and validating the rationale and all approvals. The Authorizing Agent notifies the Security Administrator of the outcome of all access requests.

The Security Administrator will set up the approved access and notify the User, the access requestor or the Authorizing Agent that access has been granted.

Review of Access
Access to UAccess Enterprise Applications will be reviewed periodically in accordance with the following procedures.

1. **Deactivation of Access for Inactive Users**
   Every six months the Security Administrator will provide the Authorizing Agent(s) with a report of all Users that have had no activity for 180 consecutive days. At the direction of the Authorizing Agent(s), the Security Administrator will survey the Inactive User’s Department Approver(s) to determine whether access of the Inactive User remains appropriate for a legitimate business need. When the Inactive User’s Department Approver indicates that access is no longer appropriate, the Security Administrator will immediately remove the access to prevent further activity. Collected survey data will be provided to the Authorizing Agent. Based on the response to that survey, the Authorizing Agent may leave unchanged, modify or terminate an Inactive User’s access. At the direction of the Authorizing Agent, the Security Administrator will process necessary access changes. An appropriate log entry will be made to note the review of the User, including the date and the action taken.

2. **Continued Appropriateness of Access**
   Annually, the Security Administrator will provide the Authorizing Agent with an extracted sample of the active User base from each UAccess Enterprise Application. At the direction of the Authorizing Agent, the Security Administrator will survey the Department Approvers to determine whether access of each User in the sample remains appropriate for a legitimate business need. Collected survey data will be provided to the Authorizing Agent. Based on the response to that survey, the Authorizing Agent may leave unchanged, modify or terminate a User’s access. At the direction of the Authorizing Agent, the Security Administrator will process necessary access changes. An appropriate log entry will be made to note the review of the User, including the date and the action taken.

3. **Review of Defined Roles When Modified**
   Whenever a defined Role or a Role’s Permissions are modified to reflect a change in business practice or system organization, each Authorizing Agent, under the direction of the Data Steward for the applicable UAccess Enterprise Application, will review its scope of access and
distribution across provisioned Users. The Authorizing Agent will notify the Security Administrator and the Users, if the review produces changes in the scope or distribution of the Role.

4. **Comprehensive Review of Roles**
Every three years, the Authorizing Agents for each UAccess Enterprise Application, will conduct a comprehensive review of all defined Roles that have not been otherwise subject to modification during the previous three-year period. This review will encompass the scope of access and distribution across provisioned Users. The Authorizing Agents will notify the Security Administrators and Users, if the review produces changes in the scope or distribution of the Role.

**Revocation of Access**
When a User leaves a position for which s/he has been granted access to an UAccess Enterprise Application, that access must be revoked as soon as practicable, as provided below.

1. **Upon a change in position**, whether for transfer, promotion, resignation, termination, or for any reason a User no longer requires access to a UAccess Enterprise Application, that User, the User’s Supervisor, the Department Approver or other responsible person should use the UAccess Access Provisioning Tool to submit a request for access removal or notify the Authorizing Agent or the Security Administrator. When necessary, the Authorizing Agent will direct the Security Administrator to revoke access. The Security Administrator will remove inappropriate access immediately upon notification. In the event of a change in position which requires different access, the Subject User’s new Supervisor or new Department Approver must request new access, as described above under the heading “Access Authorization.” The Security Administrator will notify the Authorizing Agent after the User’s access has been modified or removed.

   a. **Every two weeks**, the Security Administrator will create a report extracted from UAccess Analytics indicating Users who are no longer employees or affiliated with the University. The Security Administrator is to immediately remove access which is no longer appropriate for all such Users.

2. **Quarterly**, the Security Administrator will provide the Authorizing Agent a report indicating Users who have changed positions within the University. At the direction of the Authorizing Agent, the Security Administrator will survey the new Department Approvers to determine whether the access of each User in the report is appropriate for a legitimate business need. Collected survey data will be provided to the Authorizing Agent. Based on the response to that survey, the Authorizing Agent may leave unchanged, modify or terminate a User’s access. At the direction of the Authorizing Agent, the Security Administrator will process necessary access changes. An appropriate log entry will be made to note the review of the User, including the date and the action taken.

The Enterprise Applications Security Team will retain records of modified and deactivated access.

**Training**
Each *Data Steward, Authorizing Agent, Department Approver* and Security Administrator will obtain initial and ongoing training on the procedures for authorizing, modifying, deactivating and reviewing access.
Related Guidance
Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Access Control Standard (IS-S702)
University Employee Access to Institutional Data Policy

All italicized terms used in this standard are defined in the Information Security Terms Guideline (IS-G100).

<table>
<thead>
<tr>
<th>Revision History</th>
<th>Initial Draft</th>
<th>11/29/07</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date (version 1)</td>
<td>7/1/08</td>
<td></td>
</tr>
<tr>
<td>Revision (version 2)</td>
<td>4/7/10</td>
<td></td>
</tr>
<tr>
<td>Revision (version 3)</td>
<td>4/15/13</td>
<td></td>
</tr>
<tr>
<td>Effective Date (current version)</td>
<td>4/15/13</td>
<td></td>
</tr>
</tbody>
</table>