Scope
These procedures apply to individuals authorizing or controlling access to the University’s:

- Primary transactional enterprise business systems
  - UAccess Employee, also known as PeopleSoft Human Capital Management
  - UAccess Student, also known as PeopleSoft Student Administration systems
- EPM Data Warehouse containing various data from the transactional enterprise business systems
  - UAccess Analytics, also known as Business Intelligence

The applications by which individuals access these systems 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 Employee, UAccess Student and UAccess Analytics. It also describes requirements for training those involved in the access control process.

Definitions

- **SUBJECT USER** – A person requesting authorization or who has received authorization to access a UAccess Enterprise Application for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with the University.
- **SUBJECT USER’S SUPERVISOR** – A manager or supervisor of a Subject User. The Manager or Supervisor validates the business need for the User’s access to a UAccess Enterprise Application and requests such access on the Subject User’s behalf, describing the rationale for such access.
- **ACCESS INITIATOR** – A person who reviews requests for access to UAccess Enterprise Applications and who grants, modifies and terminates access to a UAccess Enterprise Application based on established policies and procedures. In academic units, this may be a Dean, Director or Department Chair, Head of Center or another designated person. The Access Initiator must be an authorized signer for the department, or another specifically designated person.
- **AUTHORIZING AGENT** – A person designated by the Data Steward, responsible for validating requests and approving the granting of access. The Authorizing Agent represents the interests of the Data Steward and the University, in terms of data protection.
- **ACCOUNT ACTIVATOR** – An Enterprise Applications Security Team member or other designated person responsible for the physical creation, deletion and maintenance of User access.
- **DATA STEWARD** – A person identified pursuant to the University Employee Access to Institutional Data Policy to manage the data of an Enterprise Application.
- **UACCESS ACCESS PROVISIONING** – The online system used to request access to the UAccess Enterprise Applications, and then grant or deny such requests.
- **UACCESS ENTERPRISE APPLICATIONS** – The collective representation of UAccess Employee, UAccess Student and UAccess Analytics.
• **EXECUTIVE TIER ONE, TWO AND THREE USERS** - The Users representing the top three tiers of the University organization – meaning, The University President, the President’s direct reports, and those individuals’ direct reports.

**Initial Authorization or Modification of Access**
A Subject User’s Supervisor will determine when a Subject User needs access to a UAccess Enterprise Application or when modification of a Subject User’s access to a UAccess Enterprise Application is necessary. In either case, the User’s Supervisor will acknowledge appropriate access based on legitimate business need and will relay the request for access or modification of access to the Access Initiator. The User’s Supervisor is responsible for ensuring 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.

The Access Initiator will validate 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 Access Initiator (typically, 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 Account Activator of all approved requests.

The Account Activator will set up the approved access and notify the User, the User’s Supervisor or the Authorizing Agent that access has been granted.

**UAccess Analytics – Executive Access**
The UAccess Analytics system is currently managed by the Mosaic Implementation Team, headed by a Product Manager. The Product Manager is in frequent contact with the user community and thus represents the customer facing organization. The Product Manager will therefore, help facilitate requests for access to BI Analytics. Similarly, the EA Security Team manager also help facilitate these request. Therefore, the workflow routing proposed to address the Executive, Tier One, Two and Three, access to UAccess Analytics is:

- The Analytics Product Manager requests Access to Analytics on behalf of a Supervisor and sends the request to the EA Security Team manager.
- The EA Security Team manager approves / denies the request. Approved requests are sent to the Authorizing Agent.
- The Authorizing Agent approves / denies the request. Approved requests are sent to the Security Team for final authorization/ denial and when approved for provisioning.
This solution maintains the objective of automating the process, using a system with the controls, features and audit capabilities needed to insure appropriate use of University systems and data, while insuring Tier One, Two and Three users have a viable method to obtain access.

**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 Authorizing Agent will request a report of all Users that have had no activity for 180 consecutive days. The Account Activator will distribute this report to the Authorizing Agent. The Authorizing Agent will note on the report which User’s access must be removed, then will submit the report to the Account Activator. The Account Activator will remove the access to prevent further activity.

2. **Continued Appropriateness of Access**
   Annually, the Authorizing Agent will be responsible for extracting a sample of the active User base from each UAccess Enterprise Application and surveying the Users’ Supervisors or Access Initiators to determine whether access of each User in the sample remains appropriate for a legitimate business need. Based on the response to that survey, the Authorizing Agent may leave unchanged, modify or terminate a User’s access. An appropriate log entry will be made to note the review of the User, including the date and the action taken. The Authorizing Agent will notify the Account Activator of any access changes.

3. **Review of Defined Roles When Modified**
   Whenever a defined Role and the 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 Account Activator 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, under the direction of the Data Steward 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 applicable Account Activators 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.

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 or other responsible person should notify the Authorizing Agent or the Account Activator. When necessary, the Authorizing Agent will direct the Account Activator to revoke access. The Account
Activator will remove inappropriate access immediately upon notification. In the event of a change in position that requires different access, the Subject User’s Supervisor must request new access, as described above under the heading “Initial Authorization or Modification of Access.” The Account Activator will notify the Authorizing Agent after the User’s access has been modified or removed.

Every two weeks, the Account Activator will create a report extracted from UAccess Employee indicating Users who are no longer employees or affiliated with the University. The Account Activator to immediately remove access that is no longer appropriate for all such Users.

Quarterly, the Authorizing Agent will request a report extracted from UAccess Employee indicating Users who have changed positions within the University. The Authorizing Agent is responsible for checking any reported User’s current access level to determine if access is still valid. The Authorizing Agent is responsible for continued access notations, access modification and/or removal from the UAccess Enterprise Application. The Authorizing Agent will return notification of changes to the Account Activator prior to the next scheduled report.

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

Training
Each Data Steward, Authorizing Agent, and Account Activator 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).

Revision History

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>11/29/07</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/08</td>
</tr>
<tr>
<td>Revision (numbering and hyperlinks only)</td>
<td>11/6/12</td>
</tr>
<tr>
<td>Effective Date</td>
<td>11/6/12</td>
</tr>
</tbody>
</table>