University of Missouri System
Accounting Policies and Procedures

Policy Number: APM-2.25.60

Policy Name: Security Access Validation

General Policy and Procedure Overview:

A review of PeopleSoft security access will be conducted semi-annually by the fiscal mangers identified by each Accounting Director. This review will address three major objectives:

1. Ensure that only current employees of the University Missouri have access to the accounting systems.
2. The user roles assigned to individuals is consistent with their current job functions.
3. Adequate segregation of duties is supported through the proper assignment of user roles.

Definition of Key Terms:

Authorization: One of the basic functions that, within the concept of segregation of duties, should never be combined with another segregated duty. This refers to the process of reviewing and approving transactions or operations.

Custody: One of the basic functions that, within the concept of segregation of duties, should never be combined with another segregated duty. This refers to access to or control over any physical asset such as cash, checks, equipment, supplies, or materials.

Manager: Referring to fiscal managers who may supervise persons with access to Web Applications or PeopleSoft Financial Systems. Managers are generally responsible for financial operations, reviewing transactions and validating integrity of the accounting transactions in a department. Within the context of this document, a manager is a person responsible for knowing the policies and procedures of the University and implementing internal controls within an organizational area.

Mitigating or Compensating Controls: Additional procedures designed to reduce the risk of errors or irregularities. For example, if the record keeper also performs a reconciliation process, management should perform and document a detailed review of the reconciliation and the detailed transactions; thus providing additional control over the assignment of incompatible functions.

PeopleSoft Financials Production User Access: This is a report that lists users with access to the financial system and the User Roles (or access) each user has.

Record Keeping: One of the basic functions that, within the concept of segregation of duties, should never be combined with another segregated duty. This refers to the process of creating and maintaining records of revenues, expenditures, inventories, and personnel transactions. These may be manual records or records maintained in the financial systems.

Reconciliation: One of the basic functions that, within the concept of segregation of duties, should never be combined with another segregated duty. This refers to the process of verifying the recording of transactions to ensure that all transactions are valid, properly authorized and properly recorded on a timely basis. This includes timely resolution of any differences or discrepancies identified.

Segregation of Duties: Segregation of duties is a basic, key internal control and one of the most difficult to achieve. To achieve proper segregation of duties, managers must complete a deliberate evaluation of the financial processes. Segregation of duties is used to ensure that errors or irregularities are prevented or detected on a timely basis by employees in the normal course of business. Segregation of duties provides two benefits: 1) deliberate fraud is more difficult to commit because it requires collusion of two or more persons, and 2) it is much more likely that errors will be identified. At the most basic level, no single individual should have control over two or more phases of a transaction or operation.

User Roles: Within the PeopleSoft system, user roles are those functions or system features that a person may have access to. They tell the system what a person may do within the system.

Web Applications: A user-friendly front-end interface to the University's financial systems. Thus it is also important to review access rights granted in Web Applications.

Web Applications Access: This is a report that lists persons who have access to Web Applications and what they can do within Web Applications.

Work Flow Route Control Assignments: Establishes who may initiate and who is authorized to approve a requisition. It is important to ensure there is an adequate segregation of duties and appropriate persons have these authorities.

Detail Policy and Procedure:

The ability to effect transactions and access information in the PeopleSoft system is granted through People Soft or Web Applications. Access to the financial systems should only be provided to individuals whose jobs require access to the system.

System access is controlled through the use of sign-in controls. The person's user ID and password must be registered within the system. When a user requires system access a request is submitted through the proper approval chain. Additional controls exist within PeopleSoft and Web Applications to limit a person's access to certain features and functions. The manger has responsibility to ensure system access is granted and removed when appropriate and to ensure User Roles are consistent with job roles.

Access to the financial systems must be periodically verified because staff leave, join, or change positions at the University. Managers must follow-up to ensure User Roles and WorkFlow Route Control Assignments reflect new responsibilities of staff. Since a person's responsibilities in a new position may not require the same access as their old position, managers must monitor system user roles and appropriate system access to ensure changes are made as necessary. Failure to properly assign or change PeopleSoft User Roles is a primary reason staff members share passwords—a significant control weakness.

Monthly Review:

1) Every month, the Accounting Offices receive the following reports from the IT Security Administrator:
   (a) Web Applications Access Report
   (b) PeopleSoft User Access Report
   (c) WorkFlow Route Control Assignments
2) The Accounting Office is responsible to ensure a monthly review the reports is conducted. Each Accounting Office or department manager should ensure only authorized users have access to the system and the roles assigned to each user is appropriate to their job function.
3) If changes are needed, the manager is to report the change to the Accounting Office who will facilitate the change.

Semi-Annual Review:

Twice each year a thorough and documented process is employed to provide training on certain key internal control concepts and to certify that users' access to the University's accounting systems is appropriate.

1) Accounting directors at the various campuses determine who in their campus will be responsible for performing the access reviews.
2) The Controller's Office will ensure the reviewers for each campus are provided a uniform methodology to facilitate the review and certification process.
3) The campus reviewers will:
   (a) Complete the required training
   (b) Upon satisfactory completion of the training the reviewer will review reports for the users assigned to them to ensure only authorized users have access to the system and the roles assigned to each user is appropriate to their job function.
   (c) Identify segregation of duties issues and in those instances where conflicts cannot be eliminated document the cases and the mitigating controls.
4) The Accounting Director at each campus is responsible to ensure:
   (a) All persons required to perform the review have completed it by the established deadline.
   (b) That the reviewer has certified the review is completed and there are no known control issues.
   (c) Where the reviewer has noted a segregation of duties issue, the mitigating controls are adequate to address associated risks.
5) The Controller's Office will monitor the progress of the review program:
   (a) To ensure the reviews are completed as scheduled.
   (b) All reviewers have either affirmed to the level of controls or have identified adequate mitigating controls.

RESPONSIBILITY

Accounting Directors:

- Review reports or facilitate distribution of reports to departments provided by the IT Security Manager monthly and advise of any required modifications to the users' role assignments.
- Semi-Annually, complete and document the results of a review of user role assignments.

- Where control issues exist, ensure adequate and effective mitigating controls exist and document this evaluation.
- Complete semi-annual training on the control concepts and the objectives of the access review.
- Identify and document control or segregation of duties issues and document the mitigating controls in place to mitigate associated risks.
- Responsible for administering completion of the semi-annual certification attesting to the security access review.

Fiscal Managers:

- When monthly reports are distributed to departments, the managers are to identify any control issues or lack of segregation of duties and notifying the Accounting Offices to correct access.
- Complete the semi-annual certification attesting to the completion of this review as directed by the Accounting Office.

Controller's Office:

- Monitor the semi-annual certification and reviews to ensure they are completed as scheduled.
- Where control issues are identified, review the Accounting Directors assessment of mitigating controls to ensure they are adequate and effective.

Effective Date: July 1, 2006
Revised Date: May 6, 2007

Questions and Comments?

Questions regarding interpretation and implementation of the Accounting Policy should be directed to the Campus Accounting Office. Suggested edits or revisions to the policy should be directed to the Office of the Controller.