Policy Category: PeopleSoft Financials
Policy Title: Maintaining PeopleSoft Financials Security Access

OIT establishes access to PeopleSoft for an employee based on the authorization by the employee's immediate supervisor via the *PeopleSoft Security Access Form* (Attachment A). The authorization is based on the tasks assigned to the individual and must be approved by the Application Data Steward. All employees requiring access to budget or financial data must obtain the approval of the Controller. Those employees also requesting access as Requestor or Approver for requisitioning must also attend training provided by the Procurement Office and obtain the approval of the Procurement Officer. The supervisor is also responsible for notifying OIT if the employee leaves employment with the University or if the employee transfers to another position within the University to ensure timely deactivation of access.

To provide additional assurance that access to PeopleSoft Financials is properly controlled, once each quarter (September, December, March and June) the Controller will pull a query of active accounts and submit the user names to the Office of Human Resources for confirmation of employment. The Office of Human Resources will return this list of any of these persons who are no longer employed to the Controller. The Controller will then submit this list to the PeopleSoft Security Office to have those accounts deactivated. The Controller will also deactivate user access based on the periodic e-mails from Human Resources indicating that a person has left University

Finally, to ensure that only required accounts are active on the system, the Controller will submit any user who has not signed on into his/her account within the last 90 days to the Security Officer to be deactivated. The account will be reactivated only upon submission of a memo certifying that the employee's assigned tasks require that he/she must have the access that is signed by the employee's supervisor.