# User Access Control Policy

## Summary

Implementing user access controls is one method of safeguarding computer-resident information. User access controls restrict access to authorized users and ensure that those users access only what they need to perform their duties. CSU employs user access controls to protect sensitive, critical, or valuable information from improper disclosure, modification, or deletion.

## Purpose

The goal of this policy is to ensure that CSU's information is accessible only to those users who need to access the information, and only to the extent needed to perform their duties. The critical systems that this policy pertains to are Banner and PeopleSoft.

## Policy

- An application's information owner authorizes user creation, modifications, and deletions, and assigns user permissions.
- UITS personnel cannot act as information owners. Information owners are end-users and preferably subject matter experts.
- Each application must have a designated user administrator and backup administrator. User IDs must be unique and should easily identify the user.
- Application password rules should be consistent with network password rules.
- When an employee is terminated (voluntarily or involuntarily), their application user IDs must be suspended immediately.
- Review of access controls quarterly (January, April July, October) is required.

## Procedures and Responsibilities

- The information owner is responsible for planning user access controls and must take care to assign the least access required.
- Information owners should designate a backup person to act in their absence.
- UITS personnel are responsible for performing application user maintenance and can do so only upon authority from the information owner or Human Resources (for terminations).
- The Human Resources department submits employee terminations. However, the information owner should notify the user administrator if immediate account suspension is required.
- The user administrator is responsible for documenting user access controls, while the Information Security Officer is responsible for initiating the quarterly review process. Information owners must complete the reviews in a timely fashion before the beginning of the next quarterly review.

## Related USG Policy

3.1 (IT Handbook) Information System User Account Management & 5 (IT Handbook) Information Security

## Last Update

4/17/2014

## Responsible Authority

Chief Information Security Officer