8055.00 | Change Control

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing changes to CSU information assets and provides guidance for implementing emergency changes to CSU information assets.

POLICY STATEMENT

100 Change Control
Changes to information technology systems, network resources, and applications need to be appropriately managed to minimize the risk of introducing unexpected vulnerabilities and ensure that existing security protections are not adversely impacted. Campuses must establish and document a process to manage changes to campus information assets containing level 1 or level 2 data, as defined in the CSU Data Classification Standard.

Campuses must evaluate the information security impact of changes by taking a risk-based approach to change control.

Changes to information assets which store protected data will likely require a more rigorous review than changes to non-critical assets and must be made in accordance with a formal, documented change control process. Changes that may impact the security of these information assets must be identified along with the level of control necessary to manage the change.

Campuses must define and communicate the scope of significant changes to level 1 and level 2 information assets in order to be sure that all affected parties have adequate information to determine if a proposed change is subject to the change management approval process.

200 Emergency Changes
Only authorized persons may make an emergency change to campus information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. Emergency changes are defined as changes which, due to urgency or criticality, need to occur outside of the campus' formal change management process. Such emergency changes must be appropriately documented and promptly submitted, after the change, to the campus normal change management process.