8000.00 | Introduction and Scope

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

POLICY OBJECTIVE

The CSU Information Security policy provides direction for managing and protecting the confidentiality, integrity and availability of CSU information assets. In addition, the policy defines the organizational scope of the CSU information Security Policy.

POLICY STATEMENT

100 Introduction
The Board of Trustees of the California State University (CSU) is responsible for protecting the confidentiality, integrity and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

It is the collective responsibility of all users to ensure:

- Confidentiality of information which the CSU must protect from unauthorized access.
- Integrity and availability of information stored on or processed by CSU information systems.
- Compliance with applicable laws, regulations, and CSU/campus policies governing information security and privacy protection.

The CSU Information Security Policy and Standards are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the CSU's core mission and campus academic and administrative goals.

200 Scope
The CSU Information Security policy shall apply to the following:

- All campuses.
- Central and departmentally-managed campus information assets.
- All users employed by campuses or any other person with access to campus information assets.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

Auxiliaries, external businesses and organizations that use campus information assets must operate those assets in conformity with the CSU Information Security Policy.

The CSU retains ownership or stewardship of information assets owned (or managed) by or entrusted to the CSU. The CSU reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.