8015.S000 Information Security Roles and Responsibilities

Implements:	CSU Policy #8015
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8015.0.shtml

Introduction

The CSU Information Security policy provides guidance for defining the governance structure of CSU Information Security Programs.

a) Each campus must develop, implement, and document the organizational structure that supports the campus' information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program. The governance structure must be reviewed at least annually.
b) Each President (or President-designee) and the Assistant Vice Chancellor for Information Technology Services (or the Vice Chancellor's designee) must appoint a campus information security officer (ISO). The Assistant Vice Chancellor for Information Technology Services (or the designee of the Chancellor) is responsible for the systemwide Information Security Management program and may organize the responsibilities as appropriate.

1.0 Campus President

1.1 Each CSU campus President must establish an information security program which is compliant and consistent with the CSU information security policy and standards. The details of each campus program are left to the President (or designee) to determine, with the exception of items identified in the CSU information security policy and standards; these items are meant to provide some degree of consistency of approach and application.

1.2 The President (or President's designee) must identify the specific duties and responsibilities for the ISO, which, at a minimum, include those items identified below. While the role of the Information Security Officer (ISO) may be an additional duty, the President must ensure the appointee has sufficient time to carry out the assigned duties and responsibilities.

1.3 The President may assign additional roles and responsibilities appropriate to the campus.

1.4 Each President must review information security risks at least annually.

2.0 Campus Chief Information Officer (CIO)

In addition to other duties as defined within the CSU, each campus CIO must:

a) Work with the campus ISO to develop procedures and processes which implement the CSU information security policy and standards as directed by the campus President.
b) Work with the campus ISO to evaluate the risk introduced by any changes to campus operations and systems.
c) Consult with the ISO regarding campus operations and systems to address security.

3.0 Campus Information Security Officer (ISO)

The ISO must:

a) Coordinate the campus information security program on behalf of the President.
b) Advise the President and his/her cabinet on all information security matters.
c) Work closely with campus administrators and executive officers on information security matters.
d) Oversee campus information security risk assessment activities.
e) Inform the President (or President-designee) of significant information security risks as they are identified.
f) Oversee the campus information security incident response program in coordination with appropriate campus personnel.
g) Oversee the campus information security awareness and training program.
h) Provide input to the campus budget process regarding prioritization and required resources for information security risk mitigation activities and inputs regarding information security risks of proposed projects.
i) Respond to information security related requests during an audit.
j) Serve as the campus representative on the CSU Information Security Advisory Committee.
k) Avoid conflicts of interest by not having direct responsibility for information processing or technology operations for campus programs that employ protected information.

4.0 Campus Managers

Technical and program (e.g., human resources, registrars, privacy officers, etc.,) managers are responsible for:

a) Ensuring that information assets under their control are managed in compliance with CSU and campus information security policies and standards.
b) Ensuring that staff and other users of information assets under their control are informed of and comply with CSU and campus information security policies and standards.

5.0 Campus Data Owners

5.1 The data authority/owner must:

a) Classify each information asset for which he or she has ownership responsibility in accordance with CSU and campus policies/standards, or legal, regulatory, or contractual requirements.
b) Work with the ISO to define controls for limiting access to and preserving the confidentiality, integrity and availability of information assets that have been classified as requiring such controls.
c) Authorize access to the information asset in accordance with the classification of the asset and the need for access to the information.
d) Ensure that those with access to the information asset understand their responsibilities for collecting, using, and disposing of the asset in accordance with CSU and campus policies/standards, or legal, regulatory, or contractual requirements.
e) Work with the ISO to monitor and ensure compliance with CSU/campus security policies and procedures affecting the information asset.
f) Work with the ISO to identify an acceptable level of risk for the information asset.
g) Work with the ISO, data user, data custodian/steward, and/or other authorized individuals during the investigation and mitigation of information security incidents/breaches affecting the information asset.

5.2 The ownership responsibilities must be performed throughout the life cycle of the information asset, until its proper disposal. Individuals that have been designated owners of information assets must coordinate these responsibilities with the campus ISO.

6.0 Campus Data Custodian/Steward

The responsibilities of a custodian of an information asset consist of:

a) Complying with applicable law and administrative policy.
b) Complying with any additional security policies and procedures established by the owner of the information asset and the campus ISO.
c) Advising the owner of the information asset and the campus ISO of vulnerabilities that may present a threat to the information and of specific means of protecting that information.
d) Notifying the owner of the information asset and the campus ISO of any actual or attempted violations of security policies, practices, and procedures.

7.0 Campus Data User

The responsibilities of a data user consist of:

a) Ensuring that he or she does not put any University information asset for which he or she has been given access at risk through his or her own actions.
b) Working with the ISO, data authority, data custodian/steward, and/or other authorized individuals during the investigation and mitigation of information security incidents/breaches affecting the information asset.
c) Performing as appropriate other information security duties as required by other CSU and campus policies/standards, the data owner, or the campus ISO.

8.0 Systemwide Chief Information Security Officer

The Systemwide Chief Information Security Officer must:

a) Provide leadership for the overall CSU Information Security Program
b) Conduct an periodic review and update of the CSU security policy and standards
c) Advise the Chancellor and CSU senior management on matters regarding information security
d) Provide support to information security staff at each campus
e) Develop systemwide information security strategies and metrics

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	5/20/2011	Macklin	Draft Standard	All
1.1	6/17/2011	Moske	Format draft.	All
1.2	11/5/2013	Macklin	Updated § 8 to reflect title change, added 8(e) based on feedback from ITAC. Update other section titles to distinguish between campus and systemwide personnel.	All
New	11/15/13	Moske	Accept Macklin Edits and publish final	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
Click here to enter Review Date	Click here to enter Review Date	Click here to enter Review Date
3/21/2012	ISAC	Reviewed, approved and recommended for CISO review
6/25/2013	ITAC	Reviewed and approved
11/5/2013	CISO	Reviewed and approved