8020.00 | Information Security Risk Management

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

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for the campus information security risk management program.

POLICY STATEMENT

100 Information Security Risk Management

Risk management involves the identification and evaluation of risks to information security assets (risk assessment) and the ongoing collection of information about the risk (risk monitoring). Once a risk has been identified, campuses must develop and implement strategies to reduce the risk to acceptable levels (risk mitigation), share or shift the risk to another party (risk transference), or assume the identified risk (risk acceptance).

Campuses must develop risk management processes that identify, assess, and monitor risks to information assets containing level 1 and level 2 data as defined in the CSU Data Classification Standard. Identified risks to these information assets must be actively managed by data owners and/or appropriate administrators in order to prioritize resources and remediation efforts.

200 Information Security Risk Assessment

Risk assessments are part of an ongoing risk management process. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls.

Campuses must document the scope and frequency of the assessment; risk assessment methodology; result of the risk assessment; and, mitigation strategies designed to address identified risks.

300 Information Security Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing appropriate risk-reducing activities recommended as a result of the risk assessment process. Since the elimination of all risk is impossible, campus leadership must balance the cost and effectiveness of the proposed risk-reducing activities against the risk being addressed.

Campuses must select appropriate mechanisms to safeguard the confidentiality, integrity, and availability of information assets containing protected data. Campus mitigation strategies must be commensurate with risks identified by risk assessments. For those risks where the mitigation strategy involves the use of controls, those controls must ensure that risks are reduced to an acceptable level, taking into account:

- Legal and regulatory requirements and compliance.
- Campus operation and policy requirements and constraints.
- Cost of implementation, maintenance, and operation.

Each campus must develop and maintain a process for documenting and tracking decisions related to risk mitigation activities.

400 Information Security Risk Transference

Whenever possible, a risk may be managed by sharing or completely transferring it to another entity. Campuses may transfer risks if the required actions of the receiving entity are deemed to result in an acceptable outcome should the risk be exploited and damage occurs. Risks associated with potential failure to comply with applicable laws, statutes, or regulations can only be transferred if the results will support compliance.

Each campus must develop and maintain a process for documenting and tracking decisions related to risk transference activities.

500 Information Security Risk Acceptance

Risk acceptance occurs when potential risk-reduction activities cannot be found or those identified are determined not to be cost effective (e.g. the protection measures cost more than the potential loss). In the case where resources for the best mitigation strategy are not available, the risk must be addressed to the extent possible using available resources.

Campuses must develop a process for documenting, reviewing and approving accepted risks. Accepted risks must undergo periodic review and approval by appropriate administrators.

600 Information Security Risk Monitoring

Sometimes, when a risk is identified, there may be insufficient or conflicting information regarding its likelihood of occurrence or potential impact. Campuses must monitor risks of this nature and develop a plan to gather sufficient information to judge whether the risk should be mitigated, transferred, or accepted.

700 Reporting Information Security Risks

The Senior Director of Systemwide Information Security Management must complete a risk assessment of information assets containing level 1 data as defined in the CSU Data Classification Standard at least every two years. The report must include a description of the methodology, the results of the risk assessment, and recommended systemwide mitigation strategies for addressing each identified risk. The report must be certified by the systemwide Information Security Steering Committee and presented to the Chancellor (or Chancellor-designee).