

| **Establishing an Information Security Program**

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

POLICY OBJECTIVE

The CSU Information Security policy defines minimum requirements for CSU Information Security Programs.

POLICY STATEMENT

Each campus President and the Assistant Vice Chancellor for Information Technology Services are responsible for the establishment and implementation of an information security program that contains administrative, technical and physical safeguards designed to protect campus information assets. Each campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The campus information security program reviews must be documented.

The campus program must:

- Document roles and responsibilities for the information security program.
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic).
- Develop risk management strategies to identify and mitigate threats and vulnerabilities to level 1 and level 2 information assets as defined in the CSU Data Classification Standard.
- Establish and maintain an information security incident response plan.
- Maintain ongoing security awareness and training programs.
- Comply with applicable laws, regulations, and CSU policies.