8075.00 | Information Security Incident Management

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

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing an information security incident management program.

POLICY STATEMENT

Campuses must develop and maintain an information security incident response program that includes processes for investigating, responding to, reporting, and recovering from incidents involving loss, damage, misuse of information assets containing protected data, or improper dissemination of critical or protected data, regardless of the medium in which the breached information is held or transmitted (e.g., physical or electronic). The campus program must:

- Define and/or categorize incidents.
- Designate specific personnel to respond and investigate information security incidents in a timely manner.
- Include procedures for documenting the information security incident, determining notification requirements, implementing remediation strategies, and reporting to management.
- Include processes to facilitate the application of lessons learned from incidents.
- Support the development and implementation of appropriate corrective actions directed at preventing or mitigating the risk of similar occurrences.

The campus information security incident response plans must be reviewed and documented annually and comply with the CSU Information Security Incident Management Standards.

Campus procedures must include the following notification protocol:

- If a breach of level 1 data has occurred, the campus President must notify the Chancellor, the CIO must notify the Assistant Vice Chancellor for Information Technology Services, and the campus ISO must notify the Senior Director of Systemwide Information Security Management.
- If a breach of level 2 data has occurred, the campus ISO must notify the Senior Director of Systemwide Information Security Management. The Senior Director will provide the Chancellor with quarterly status reports on level 2 data breaches that have occurred in the CSU.