8045.00 | Information Technology Security

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

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing information technology security and guidance for: monitoring CSU information assets; protecting information assets from malicious software; and managing network security and mobile devices.

POLICY STATEMENT

100 Information Technology Security

Campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

200 Protections Against Malicious Software Programs

Each campus must have plans in place to detect, prevent, and report malicious software effectively. Electronic data received from untrusted sources must be checked for malicious software prior to being placed on a non-quarantined location on a campus network or information system.

300 Network Security

Campuses must appropriately design their networks—based on risk, data classification, and access—in order to ensure the confidentiality, integrity and availability of their information assets. Each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

400 Mobile Devices

Campuses must develop and implement controls for securing protected data stored on mobile devices. Protected data must not be stored on mobile devices unless effective security controls have been implemented to protect the data. Campuses must use encryption, or equally effective measures, on all mobile devices that store level 1 data as defined in the CSU Data Classification Standard. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by a designated campus official. Other effective measures include physical protection that ensures only authorized access to protected data.

500 Information Asset Monitoring

Campuses must implement appropriate controls on the monitoring of information systems and network resources to ensure that monitoring is limited to approved activities. Monitoring must not be conducted for the purpose of gaining unauthorized access, “snooping”, or for other activities that violate the CSU Responsible Use Policy. Records created by monitoring controls (e.g. logging) must be protected from unauthorized access and reviewed regularly. Campuses must ensure that only individuals who have a “need-to-know” are granted access to data generated from monitoring controls.

Data generated by monitoring must be retained for a period of time that is consistent with effective use, CSU records retention schedules, regulatory, and legal requirements such as compliance with litigation holds.
At a minimum, server administrators are required to scan regularly, remediate, and report un-remediated vulnerabilities on critical systems or systems that store protected information within a prescribed timeframe. The risk level of a system determines the frequency at which logs must be reviewed. Risk factors to consider are:

- Criticality of business process.
- Information classification associated with the system.
- Past experience or understanding of system vulnerabilities.
- System exposure (e.g., services offered to the Internet).