8060.00 | Access Control

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

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing access to CSU information assets and guidance for: granting access to CSU information assets; separating duties of individuals who have access to CSU information asset; conducting reviews of access rights to CSU information assets; and modifying user access rights to CSU information assets.

POLICY STATEMENT

100 Access Control

On-campus or remote access to information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard must be based on operational and security requirements. Appropriate controls must be in place to prevent unauthorized access to protected information assets. This includes not only the primary operational copy of the protected information assets, but also data extracts and backup copies. Campuses must have a documented process for provisioning approved additions, changes, and terminations of access rights and reviewing access of existing account holders. Access to campus protected information assets must be denied until specifically authorized.

Access to public and shared resources may be excluded from this requirement. Campuses are required to identify and document public or shared resources that are excluded from this requirement. Authorized users and their access privileges must be specified by the data owner, unless otherwise defined by CSU/campus policy.

200 Access Control

Access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of need-to-know and least privilege.

Authentication controls must be implemented for access to campus information assets that access or store protected data, must be unique to each individual and may not be shared unless authorized by appropriate campus management. Where approval is granted for shared authentication, the requesting organization must be informed of the risks of such access and the shared account must be assigned a designated owner. Shared authentication privileges must be regularly reviewed and re-approved at least annually.

300 Separation of Duties

Separation of duties principles must be followed when assigning job responsibilities relating to restricted or essential resources. Campuses must maintain an appropriate level of separation of duties when issuing credentials to individuals who have access to information assets containing protected data. Campuses must avoid issuing credentials that allow a user greater access or more authority over information assets than is required by the employee’s job duties.

400 Access Review

Campuses must develop procedures to detect unauthorized access and privileges assigned to authorized users that exceed the required access rights needed to perform their job functions. Appropriate campus managers and data owners must review, at least annually, user access rights to information assets containing protected data. The results of the review must be documented.

500 Modifying Access

Modifications to user access privileges must be tracked and logged. Users experiencing a change in employment status (e.g., termination or position change) must have their logical access rights reviewed, and if necessary, modified or revoked.