8030.00 | Personnel Information Security

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

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing personnel information security, defines pre-employment requirements, and provides guidance for managing separations or changes in employment status.

POLICY STATEMENT

100 Personnel Information Security

All users are expected to employ security practices appropriate to their responsibilities and roles. Users who access level 1 or level 2 data as defined in the CSU Data Classification Standard must sign an approved system-wide confidentiality (non-disclosure) agreement.

200 Employment Requirements

Campuses must develop procedures to conduct background checks on positions involving access to level 1 information assets as defined in the CSU Data Classification Standard.

300 Separation or Change of Employment

Campuses must implement procedures to revoke access to information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy and by the data owner. Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical, and remote access, must be promptly revoked.

Procedures must be implemented to ensure proper disposition of information assets upon termination. Electronic and paper files must be promptly reviewed by an appropriate manager to determine who will become the data steward of such files and identify appropriate methods to be used for handling the files. If the separating employee is holding resources subject to a litigation hold, the campus must ensure preservation of relevant information until the litigation hold has been revoked, at which point the resource is subject to the normal record retention schedule.

Campuses must verify that items granting physical access such as keys and access cards are collected from the exiting employee. Any access list that grants the exiting employee physical access to a limited-access area on the campus must be updated appropriately to reflect the change in employment status.

Each campus must establish procedures to allow for separated employees to obtain such incidental personal electronic information as appropriate.

Information system privileges retained after separation from the campus must be documented and authorized by an appropriate campus official.