CSU

ICSUAM

Section 7000

Identity Access Management

Table of Contents

7100.00 | Identity Access Management

Effective Date: 4/28/2014

POLICY OBJECTIVE

The CSU Information Security Policies (§ 8000) require secure, reliable and timely methods to control access to information assets. Identity Access Management (IAM) is a framework that consists of governance, process, and technology to control access to information, systems, and physical resources using Electronic Identities. This policy identifies the responsibilities of CSU Campuses and the Chancellor's Office related to Identity and Access Management.

POLICY STATEMENT

100 Governance

CSU Campuses and the Chancellor's Office must establish an Identity and Access Management program. The Campus Identity and Access Management program must identify responsibilities for governance of electronic identity records and associated business processes.

Campus Identity and Access Management governance must encompass the full life cycle of identities and electronic identity records from creation through modification and revocation. Information authorities (Data Owners) must be identified for each affiliate type that is issued an electronic identity record.

Each campus must maintain written procedures for managing campus issued electronic identity and associated account information.

Campus procedures must:

- identify authoritative data sources and data owners of identity information (e.g. CMS records),
- designate who can create and update identity information within an electronic identity record,
- ensure that identity records for active affiliates are accurate, complete, and contain current information, and changes are logged,
- and designate the individuals accountable for maintaining the integrity of the Identity Access Management System (IdAMS).

Campus governance decisions and standards related to identity management must adhere to systemwide IAM program definitions attached to this policy.

Each campus must participate in the CSUconnect Identity Federation, adhere to CSUconnect Federation standards, and maintain annual membership with InCommon.

200 Electronic Identity Records

Each CSU campus must maintain an authoritative Identity Registry (IR) that manages electronic identities, identity records, and associated account names. Electronic identities must be assigned to a real person and must never be reissued. User Accounts (e.g. Network ID) must be associated with a single Electronic Identity.

300 Electronic Credential Issuance and Identity Verification

Level of Assurance defines the procedures to establish the level of certainty between a unique person and their Electronic Identity. Every Electronic Identity record must have a level of assurance assigned to it.

An Electronic Credential (e.g. an account with a secret password) is used to electronically authenticate a person's Identity. Credential issuance processes must meet the appropriate NIST Level of Assurance and must be done in accordance with the Access Control Policy (8060) and Standard.

400 Level of Assurance for Access Control

Use of Electronic Identity for access must follow the Access Control Policy and Standard (8060). The Identity verification and Electronic Credential issuance process must be consistent with NIST Level of Assurance (LOA) 2 before an Electronic Identity must be used to access Level 1 data and must be consistent with LOA 1 when used to access Level 2 data.

500 Affiliation
CSU systemwide affiliations are defined by systemwide Identity Access Management in coordination with the appropriate governing authority. Campus-wide affiliations must be defined through local campus governance. Changes in a person's affiliations and status must be accurately reflected in the IdAMS.

APPLICABILITY AND AREAS OF RESPONSIBILITY

This policy applies to the Chancellor's Office and all 23 CSU campuses.