## 8060.S000 Access Control

| | |
|---|---|
| **Implements:** | CSU Policy #8060.0 Access Control |
| **Policy Reference:** | http://www.calstate.edu/icsuam/sections/8000/8060.0.shtml |

## Introduction

Access to campus information assets containing protected data must include a process for documenting appropriate approvals before access or privileges are granted. All changes to user accounts (i.e., account termination, creation, and changes to account privileges) on campus information systems or network resources (except for password resets) must be approved by appropriate campus personnel. Such approval must be adequately documented in order to facilitate auditing of access control practices.

## 1.0 Access Authorization

Campuses must identify and document individuals who are authorized to define and approve user access to campus information assets. Campuses must document their authorization procedures. Authorizations must be tracked and logged following campus defined processes and must include information appropriate to the nature of the data stored on the information asset. Information should include:

a) Date of authorization

b) Identification of individual approving access

c) Description of access privileges granted

d) Description of business reason for which access privileges were granted

### 1.1 Granting Access

Authentication controls must be implemented for campus information assets which store or access protected information, and for systems the campus considers critical to operations. Campus-defined controls must take into consideration:

a) The need to validate user identity prior to granting access to protected data.

b) The requirement for unique user accounts and corresponding access privileges.

c) The requirement to deny all access rights until rights are formally approved and assigned.

d) The ability to report repeated failed access attempts.

e) The ability for access rights to be promptly modified or revoked.

f) The need for authentication credentials to be regularly changed.

### 1.2 User Account Management

a) Unless otherwise authorized, all users of campus information assets must be identified with a unique credential that establishes identity. This unique credential must not be shared with others except where authorized as an exception to this standard. User credentials must require at least one factor of authentication (e.g., token, password or biometric devices).

b) Campuses must establish criteria for expiring, disabling, and removing user accounts on critical systems and campus information systems or network resources that store or access protected information. The period of acceptable inactivity must be based upon the nature of the data and/or the criticality of the system.

c) "Guest" or generic accounts on campus information systems or network resources may be activated only when authorized by appropriate personnel. Any such account created on a critical system must be reported to the campus information security officer.

d) Campuses must establish processes for re-enabling or resetting user accounts once they have been disabled. User identity must be appropriately verified prior to re-enabling or resetting user accounts.

e) System administrators of campus information systems and network resources must have individual user accountability on the information systems and network resources they administer or use protected utilities to perform system administration tasks. System administrator accounts must not be used for non-administrative uses (e.g., browsing the Web while logged in as administrator).

f) Campuses must establish criteria for creating application or system-level access accounts. These accounts must be assigned appropriate stewards and reviewed at least annually.

1.3 Password Management

a) Campuses must identify and implement password criteria which meets NIST Level 1 "Resistance to Guessing Authentication Secret"1 at a minimum. To prepare for InCommon Bronze/Silver implementation, campus should consider meeting NIST Level 2 for "Resistance to Guessing Authentication Secret". Password criteria involves a combination of minimum password length and complexity, password aging, exclusion of dictionary words, and account locking based on failed authentication attempts. Refer to NIST Special Publication 800-63-2 [SP 800-63-2], for a discussion of Authentication Secret complexity and resistance to online guessing. See Appendix A for examples of compliant password criteria and a link to a complexity calculator.

- Complexity: Campuses must implement password complexity standards sufficient to protect against password guessing.
- Failed Attempts: Campuses must identify criteria for disabling (locking) user accounts on critical campus information assets after a number of failed logon attempts, and acceptable timeframes to maintain a disabled state.
- Aging: Campuses must identify and enforce a password change (aging) schedule. The schedule may vary by system or application at the campus' discretion as determined by risk.

b) Critical information systems and those with protected data should use a secure external authentication method, such as a campus directory server.

c) Passwords and credentials that grant access to Level 1 and Level 2 data must not be used as credentials for personal (non CSU) accounts.

d) Password Issuance – When passwords are issued they must be One-Time Passwords/Keys. One-Time passwords (e.g., passwords assigned during account creation, password resets, or as a second factor for authentication) must be set to a unique value per user and changed immediately after first use.

[1] At present, this publication can be located on line at http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-2.pdf

1.4 Password Storage and Transmission

a) Passwords or credentials that grant access to level 1 and level 2 data are classified as level 1 data by the CSU data classification standard. When transmitted electronically, they must be sent via a method that uses strong encryption as per the CSU Information Security Asset Management Standard.

b) All other user account passwords should be protected with strong encryption during storage and transmission.

c) Strong encryption or hash methods must be used to protect any passwords stored in a collection of passwords (database).

d) Campuses may identify service accounts or other low risk applications where password storage or transmission in clear text is appropriate.

## 2.0 Access Modification

At least annually, appropriate campus managers, data stewards, and/or their designated delegates must review, verify, and revise as necessary user access rights to campus information assets which store or access protected data. All such revisions must be tracked and logged following campus defined processes and must at least include:

a) Date of revision

b) Identification of person performing the revision

c) Description of revision

d) Description of why revision was made

## REVISION CONTROL

**Revision History**

| Version | Revision Date | Revised By | Summary of Revisions | Section(s) Revised |
|---|---|---|---|---|
| 1.1 | 9/1/2011 | Macklin | Incorporate ISAC comments | all |
| 1.2 | 10/11/2011 | Macklin | Incorporate ISAC comments | 1.1 – 1.3 |
| 1.3 | 6/1/2012 | Arboleda/Harwood | Incorporated CalPoly Pomona comments and Auditor Concerns | 1.0, 2.2, 2.3 |
| 1.4 | 6/4/2012 | Macklin | Comments to v1.3 | All |
| 1.5 | 6/5/2012 | Harwood/Macklin | Final Draft | All |
| 1.6 | 3/11/2013 | Hendricks | Draft Revision Password Mgmt | 1.3 |
| 1.7 | 5/2/2013 | Macklin | Incorporated comments, Created Appendix A | Primarily 1.3 |
| 1.8 | 5/7/2013 | Macklin/Hendricks | Incorporated comments | 1.3. 1.4 |
| 1.9 | 5/15/2013 | Macklin | Incorporated comments | 1.3(a)(1), 1.3(b) |

**Review / Approval History**

| Review Date | Reviewed By | Action (Reviewed, Recommended or Approved) |
|---|---|---|
| 6/5/2012 | Macklin | Reviewed/Approved |
| 6/5/2012 | Perry (CISO) | Approved |
| 5/21/13 | ISAC | Recommended Updated Draft |
| 6/5/13 | ITAC | Review |
| 7/16/13 | Perry (CISO) | Approved for Posting |