CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Access Control Standard
Information Technology Services

Last Revised: **03/15/2021**

Approved: **04/12/2021**

REVISION CONTROL

Document Title: CSUSB Access Control Standard

Author: Javier Torner

File Reference:

Date	By	Action	Pages
05/18/2006	J Torner	Created Standard	All
04/06/2010	J Torner	Revised Standard	All
02/10/2015	L Carrizales	Revised Standard	All
03/10/2015	L Carrizales	Revised Standard	All
04/22/2015	L Carrizales	Standard approved by ISET Subcommittee	All
08/29/2016	L Carrizales	Added Multi-Factor Authentication requirements & Updated Password Controls	Section 7, 8 and 9
09/08/2020	G Au	Revised Standard	All
03/15/2021	G Au	Revised MFA requirements	Section 7

Review/Approval History

Date	By	Action	Pages
2/15/2017	IT Governance ISET Subcommittee	Approved Recommendations	All
10/12/2020	IT Governance ISET Subcommittee	Approved Revisions	All
04/12/2021	IT Governance ISET Subcommittee	Approved Revisions	

1.0 Introduction

CSUSB is responsible for protecting and securing information assets, including systems, infrastructure and data under its control. In order to satisfy our responsibility to protect the confidentiality, integrity and availability of these information assets, CSUSB has adopted the following standard, procedures and guidelines to ensure that only authorized users and systems have access to critical systems, information and infrastructure. Critical information assets are identified as such through the risk assessment process commensurate to the campus Information Asset Management Standard.

2.0 Scope

This standard applies to all university systems that contain protected information or have access to protected Level 1 and Level 2 information as defined by the CSUSB Information Classification Standard, as well as systems or equipment that is critical for campus operation or infrastructure. Anyone who has access to these information assets whether in electronic or physical form, including faculty, staff, students, vendors or other affiliates is subject to and has responsibilities under this standard.

3.0 User Responsibilities

University administrative information systems and data are for use only by the individual granted access.

Users must:

- Only use administrative information systems for the sole purpose of conducting official University business.
- Access to administrative information systems is based on their need to use specific data, as defined by job duties, and is subject to appropriate approval.
- Comply with state and federal laws; CSU policies; and University standards, guidelines and procedures that govern access to and use of Level 1 confidential data and Level 2 internal use data, regardless of its format.
- Follow the recommendations of the CSUSB Safeguarding Confidential Information Standard.

Users may not:

- Disclose data to others, except as required by their job responsibilities.
- Use data for their own personal gain, nor for the gain or profit of others.
- Access data to satisfy their personal curiosity.

4.0 Granting and Revoking Access

Access to information assets requires the authorization from the information authority or data custodian responsible for granting access to the system or data. A delegation of authority must be in place in situations where the information authority or data custodian has assigned their responsibilities to another individual as required by the CSUSB Information Authorities and Custodians Standard.

Information authorities and data custodians are required to establish and document the access criteria for account eligibility, creation, and expiration. All access granted, modified or revoked must be documented.

All access to protected Level 1 and/or Level 2 information assets must be denied until specifically granted.

No access shall be granted until authorized by the appropriate information authority or data custodian.

All access privileges must be based on the required duties and responsibilities of each user or system.

In situations where it is necessary to grant access between applications and systems or to grant access to classes of users, appropriate access controls should be implemented to ensure that authentication credentials and information assets are sufficiently protected.

Access must be removed or modified in a timely manner when it is no longer required.

5.0 Reviewing Access

Information authorities and data custodians should regularly review all access to the information assets under their control to verify the continued need for access.

Access controls should include mechanisms to detect and warn about repeated failed access attempts.

Information authorities and data custodians must regularly review system access logs to ensure that no unauthorized access is taking place.

All instances of non-compliance with this standard including all unauthorized access must be immediately reported to the campus Information Security Officer.

System logs must be kept for a minimum of 180 days or for a time as required in the campus data retention schedule.

6.0 Network Access Control

Network access controls should adhere to the CSUSB Network Security Management Standard.

Information authorities and data custodians should follow the CSUSB Network Security Management Standard for the addition and/or removal of critical information assets on protected network segments. All changes must be approved by the appropriate information authority and/or data custodian.

Information authorities and data custodians should review appropriate logs to ensure the continued security of the network.

Appropriate network access control, such as the use of VPN and/or multi-factor authentication, must be required for remote access to information assets that contain, process or access protected information.

7.0 User Authentication and Password/Passphrase Management

7.0.1 User Authentication

Information assets must be protected by an authentication mechanism that allows users and their corresponding privileges to be uniquely identified. Examples may include traditional system passwords, challenge response systems, hardware tokens and PKI certificates.

All users who have access to protected Level 1 data, significant amounts of Level 2 data or have administrative access to critical university systems or systems containing protected data are required to use multi-factor authentication.

Authentication credentials, including passwords, must be of sufficient strength and complexity to adequately protect the information assets under its control.

Authentication credentials must be protected from unauthorized disclosure. This includes, for example, using encrypted authentication mechanisms when accessing information resources over a network.

Authentication credentials must be unique to each individual and must not be shared unless approved by the appropriate information authority or data custodian.

In cases where shared authentication credentials are required for a non-interactive task or database, access must be limited and unique to a specific application or function and approved by the appropriate information authority or data custodian.

Authentication credentials must be changed as appropriate on a regular basis. All authentication credential standards must be documented and automatically enforced by appropriate mechanisms.

Authentication credentials must be changed or revoked in a timely manner when user job responsibilities or employment status changes.

Information authorities and data custodians should have a notification and reset procedure for lost, forgotten and compromised authentication credentials including an escalation process for critical information assets.

7.0.2 User Password or Passphrase

All campus users must be provided with a unique set of credentials that establishes their identity. User credentials must require at least one factor of authentication, such as a password or passphrase. Passwords/passphrases are commonly used mechanisms to verify a user's identity before providing access to an information system or service.

Users are responsible for keeping their authentication credentials confidential, as well as for all transactions performed using their credentials.

7.0.3 Multi-Factor Authentication

Multi-Factor Authentication (MFA) is required for all CSUSB Single Sign On systems where applicable. The purpose of using MFA is to create one more layer of defense to prevent unauthorized access to protected information. The addition of MFA becomes more critical as the university has adopted using Single-Sign-On authentication, that is, a single set of credentials that provide access to all authorized university systems and applications.

MFA adds a step in the login process and requires the individual to validate their identity after entering their login credentials by responding to a prompt using a second factor, such as a mobile device (iPhone, Android, Tablet, iPad, etc.), or hardware token.

8.0 Passphrase Requirements

Users are required to construct their password/passphrase based on the following minimum requirements:

1. Password/Passphrase Complexity

- Minimum of 12 characters (longer is generally better)
- At least one character from each of the following:
- One Upper case letter (A-Z)
- One Lower case letter (a-z)
- One Special Character (non-alphanumeric)
- One Numeric character (0-9)

2. Password/Passphrase Restrictions
    - 50 previous passphrases cannot be reused
    - Cannot include your account name
    - Cannot include a word normally found in the dictionary
    - User account is locked after 10 failed login attempts
    - The lockout from failed attempts is released after 30 minutes

For other systems, users should follow the recommended procedure established by the information authority or data custodian.

If a university system has limitations that do not meet the password/passphrase minimum requirements or there is a need for a higher level of security, then the information authority or data custodian must specify password/passphrase requirements and a corresponding change schedule based on a risk assessment.

9.0 Compromised Credentials

Credentials that have been or are suspected to have been compromised should be changed immediately. Users should immediately report to the Information Security Office any incident in which they suspect someone else may be using their credentials or may be accessing their account.