
Process Number: BP-05-003
Approved By: A. Michael Berman
VP for Technology & Innovation

Effective Date: 05/08/2017
Page 1 of 2

Business Practice for Access Controls

PURPOSE:

Provide support of [ICSUAM Policy 8060.200](#) for Access Control.

BACKGROUND:

To support [ICSUAM policy 8060.200](#), 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 or information systems and services that access or store protected data, and 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.

BUSINESS PRACTICE:

Accountability:

Vice President for Technology and Innovation
Information Security Officer

Applicability:

All systems and services containing protected level 1 confidential data

Definitions:

Multi-Factor Authentication – a method of computer access control in which a user is granted access only after successfully presenting several pieces of evidence to an authentication mechanism, typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

Process Number: BP-05-003
Approved By: A. Michael Berman
 VP for Technology & Innovation

Effective Date: 05/08/2017
Page 2 of 2

Business Practice for Access Controls

Two-Factor Authentication (or 2FA) – is a method of confirming a user’s claimed identity by utilizing a combination of two different components. Two-factor authentication is a type of multi-factor authentication.

Text:

General

To promote stronger access controls to protect CI systems and services containing protected level 1 confidential data, CI shall implement multi-factor authentication in addition to its current access control security practices for users accessing protected level 1 confidential data. Multi-factor authentication will add the additional authentication layer of something you have to the existing “something you know” (e.g. password and user id). This combined authorization control will help to better protect CI’s information assets and prevent credential fraud.

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned
Assessment of business practice	Annual	ISO

Revision History

BP Nbr:	BP-05-003	Enacted Date:	
Revision Nbr:	999	Revision Date:	99/99/9999
		Revised By:	