1.0 Introduction

This standard provides the requirements for validating the identity of employees, students and others who require access to protected information. For a campus to make the linkage between a claimed identity and real-life existence of a person, they need valid forms of identity evidence, and to verify that the individual to be identified matches that identity evidence. There are three main steps to the identity verification process, the first is the acceptability of the identity proof, the second is validation of the identity, and the third is verification of identity.

"Acceptability of the identity proof" addresses what form of identity evidence is allowed, how much information is required, and the required strength level of that evidence.

"Validation of the identity" is the process of confirming that the provided identity evidence is not fraudulent.

Lastly, "verification of identity" is the process of confirming that the individual identified by the evidence is the individual who is offering the evidence.

Determination of the "identity assurance level" necessary to protect the assets to be accessed will inform the strength of the acceptability, validation and verification processes.

Implements: CSU Policy ICSUAM 8060.0 Access Control

Policy Reference: https://csyou.calstate.edu/Policies/icsuam/Pages/8060-00.aspx

2.0 Definitions

Level of Assurance (LOA) – a term used in NIST 800-63-2[1], and still in common use, which indicates the degree of confidence needed to establish an identity. Example: LOA2 requires some confidence in the user's identity and may be implemented via a single authentication factor, typically a password. LOA3 requires high confidence in the user's identity and may be implemented with both a password and an approved authenticator.

[1]NIST Digital Identity Guidelines may be found at https://www.nist.gov/itl/tig/projects/special-publication-800-63

Authenticator Assurance Level (AAL) – a term used by NIST 800-63-3 which indicates the extent to which a user controls the authenticator bound to their account. Example: AAL2 provides high confidence that that the user controls the authenticator.

3.0 Identity Verification Principles

1. A password, token or other element of identity proof may not be issued, changed or reset without identify verification. Example: A campus may not reset a user's password, without the acceptability, validation and verification steps required to determine that the individual requesting the password reset is the individual associated with the account.

2. The identify verification process must include ability for remote (not in person) verification.

3. The identity verification process must protect against fraud from people associated with the user requesting verification (e.g. family members, roommates, employers, etc.), as these people may know the answers to verification questions.

4. The identity verification process must require that only the minimum amount of info necessary to verify identity is revealed to verifier. For example, use of a strong evidence of identity such as personal presentation of an official photo ID card is adequate, without requiring the user to also provide other identity elements such as phone number, address, etc.

5. When using "information known by the requestor" to validate identity, the campus must rely only on previously known data, and not on information provided by the user during the validation process.

6. Caller ID, along with email addresses which incorporate the users first and/or last name may not be used as an evidence of identity.

4.0 Identity Verification Criteria

4.1 Verification requirements

Verification processes must be designed to limit the exposure of the PII to the minimum necessary to establish the unique identity characteristics of the user.

4.2 Campuses must develop and maintain a method for initially establishing identity which:

a) requires verification of identity using acceptable identity proof as described under "Evidence of Identity" below,
b) may include taking a photograph for use when later reestablishing identity of the user,
c) may include issuing a campus identity card, and
d) may include electronically recording biographic/demographic data.

4.3 Campuses must develop and maintain a method for reestablishing identity using acceptable identity proof as described under "Evidence of Identity" below.

5.0 Evidence of Identity

5.1 Acceptability of Identity Proof

1) One Superior Piece of identity
   or
2) Two Strong Pieces of identity
   or
3) One strong and two pieces of fair identity

5.2.1 Validation of Identity Proof

Evidence used to provide identity must be able to be used by the identity verifier in that it must be

a) Unexpired
b) written in a language readable by the verifier
c) In such condition for writing to be legible, or photos suitable for visual verification

Identity Evidence	Examples
Superior	In-person presentation of government issued photo ID such as driver's license or passport, or campus identification.
Strong	Comparison of the photo image of the user previously taken for identity purposes with the user's appearance in a live video call Or Verification of a government photo ID or student ID over a live video call. (NOTE: An image containing a government ID is Level 1 data and must be protected appropriately at all times, including during transfer from user.)
Fair	Confirmation via recovery email. User must be able to provide answers to identity validation questions including but not limited to place of birth, mother's maiden name, etc. Users must be able to provide answers to academic record or employment questions verifiable by the identity verifier

5.3 Disabling recovery methods

Campuses must implement a method to allow users to disable online recovery methods for their individual accounts.

6.0 Identity Verification Activity Records

When identity verification activities resulting a change of credential password/token or other grant of access or protected information, a record of the activity must be made. These records must be maintained for a minimum of three years.

Identity verification activity records must contain:

- Date/time
- Identity being verified
- Verification method
- Resulting action, e.g. “password reset” or “record updated” or “denied – unable to verify”
- Organization or office performing the validation, e.g. “HelpDesk” or “Financial Aid”
- Identity of verifier
- Purpose of verification, e.g. “Password change” or “Financial Aid query”

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
11/17/2020	Mark Hendricks, Interim VP/CIO	Recommended.
1/14/2021	ISO Team, IDM Team, Servicedesk	Reviewed.
2/5/2021	AITC	Presented to AITC for review/comments.
2/22/2021	IRT, AITC	Receive comments/feedback from AITC.
2/23/2021	Admissions Office, Office of the Registrar, Bursar’s Office, Financial Aid	Reviewed.
3/1/2021	Human Resources, Payroll, Benefits	Reviewed.
3/1/2021	IRT, Director of Policy and Records Management	Recommended for approval/publication.
3/8/2021	Cabinet	Approved.