1.0 Introduction

Campuses must protect the confidentiality and integrity of CSU systems and the data stored in them. Level of assurance for authentication is a term used to address the technical and administrative controls used to ensure that an individual is who they say they are. A higher level of assurance, and technical requirements, are required based on the sensitivity of the data that individual has access to. This may be accomplished via use of a password that meets established levels of complexity along with other factors such as use of multi-factor authentication devices as necessary to protect the information asset. Risk assessment methodologies may be used to identify the level of assurance required to ensure that the person accessing an information asset is in fact the individual authorized to do so. In general, access to protected level 1 information requires a level of assurance that includes both a password and another factor such as an authentication device. Access to protected level 2 data requires a password complexity that meets minimum requirements so as to avoid guessing or common brute force attacks. While not required for access to individual Level 2 records, multi-factor authentication is recommended to prevent account compromise.

Although in general, the CSU uses ISO 27001 as a framework, in certain situations the NIST standards are used to specify technical controls. In September of 2017, NIST released 800-63-3, a comprehensive authentication and assurance guidance digital identities. In version 63-3, there is a philosophical shift away from a reliance on password complexity and towards reliance on multi-factor authentication technologies. Sacramento State has adopted a Multi-Factor-Authentication strategy for remote authentication which will meet NIST 800-63-3.

Implements: CSU Policy ICSUAM 8060.0 Access Control

Policy Reference: User Access Review Procedure for Level 1 Systems

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.

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.

2.0 Assurance Criteria

Protected Level 1 data requires use of authentication methods that use both a secure password and an authenticator. These methods must meet NIST 800-63-3 AAL2 in that they require both a secure password and use of a authenticator, for example, push technology or software token (ex: authenticator app), RSA key, etc. Sacramento State uses secure and complex passwords meeting the requirements of NIST 800-63-3. Examples of this campus standards are described in § 3.0.

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

3.0 Password Criteria Standard

For 800-63-3, assurance relies less on complex passwords and more on MultiFactor Authentication.	**Model NIST 800-63-3 example complexity rule set**	**Sacramento State Implementation/Standard**
Complexity:	Minimum password length of 10 characters On creation, password must not contain • Password obtained from previous breaches • Dictionary words • Repetitive or sequential characters Context-specific terms (username, campus, etc)	Complexity: None Not contain more than 3 consecutive same characters Not contain context-specific and campus-related and common dictionary words
Failed Attempts:	After 10 failed attempts, account is locked for 5 minutes; or User is required to complete a CAPTCHA be attempting authentication again	Campus Authentication: Duration: 1 minute Threshold: 60 failures Observation (lock): 1 minute Password Portal Authentication: Duration: None - accumulative Threshold: 10 failures Observation (lock): None - must be reset by Service Desk.
Aging:	One year expiration	Three-year expiration with Multi Factor Authentication(MFA) One-year without MFA
Multi-factor authentication:	Required use of approved authenticator device	Required (Duo) for all person-type and admin-type accounts.

4.0 Authentication methodology implementation

1) Critical information systems and those with protected data must use a secure authentication method such as a campus directory server.

a) Where authentication by campus directory is not possible, (i.e. cloud-based application which does not integrate with campus authentication methods), the system must be configured to ensure that the accounts used are adequately provisioned, de-provisioned and access follows the philosophy of least privilege.

b) The password and assurance criteria from § 3.0 still apply.

2) When passwords are issued they must be One-Time Passwords/Keys. One-Time passwords (e.g., passwords assigned during account creation, password resets), must be set to a unique value per user. The user must be provided instructions to change the issued password immediately after first use.

3) The campus multifactor authentication methodology implemented must:

a) Require a periodic re-authentication within a maximum of 12 hours.

b) Limit user-selectable "remember-me" features to a maximum of 24 hours.

4) Remote requests for password reset and/or multi-factor authenticator bypass must be requested, logged and recorded in the campus ticketing system.

a) Campus method must include identify verification consistent with ICSUAM 7100.

b) Requests for password reset and/or multifactor authenticator bypass must be logged.

c) Records of request must contain requesting account, date, request method, identity verification method, support staff identity and outcome.

d) Records of requests must be retained in the campus ticketing system.

5.0 Password Storage and Transmission

1) Strong encryption must be used to protect passwords stored in a collection of passwords (database)[2].

2) Service accounts or other low risk applications where password storage or transmission in clear text is necessary must be logged and tracked via the ticketing system. The risk associated with these accounts must be mitigated by compensating controls as per risk assessment.

6.0 Authentication Assurance Requirements

1) NIST 800-63-3 has adopted a philosophy that the password as a single factor is not secure, and has recommended the use of more than one factor for all authentication assurance levels. Implementation of multifactor authentication within an organization is addressed in NIST 800-63-3. Multi-factor authentication methods for the following are required:

a) Remote (i.e. off campus) access to protected level 1 information (i.e. CMS) which applies to another individual.

b) Access to internal campus network resources via VPN

c) Critical access, for example - have administrative access to critical operational systems (i.e. admin access to firewalls).

[2] See NIST 800-63-3-B § 5.1.1.2

2) Account compromise: In order to protect against employee account compromise a combination of controls which may include methods such as the following is required:

   e) Multifactor authentication for access to designated campus resources (e.g. VPN) from off campus with max 12 hours period

   f) Restrictions on access based on geographical locale, host profile (i.e. global protect) or other technical solution

   g) Monitoring for access from multiple locations within a specified amount of time.

   h) Awareness training designed to prevent phishing and/or other methods of credential compromise

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
11/17/2020	Mark Hendricks, Interim VP/CIO	Recommended.
1/5/2021	ISO Team, IDM Team	Reviewed.
1/12/2021	ISO Team, IDM Team	Reviewed - Incorporate feedback, update draft.
1/19/2021	ISO Team, IDM Team	Reviewed - Incorporate feedback, Update draft.
2/5/2021	AITC	Presented to AITC for review/comments.
2/22/2021	IRT, AITC	Receive comments/feedback from AITC.
3/1/2021	IRT, Director of Policy and Records Management	Recommended for approval/publication.
3/8/2021	Cabinet	Approved.