UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

UC Account and Authentication Management Standard

Revision History

Date:	By:	Contact Information:	Description:
06/08/18	Robert Smith	robert.smith@ucop.edu	Initial issue of the Standard. Approved by the CISOs for consideration by ITLC and shared governance. Interim until approved by ITLC.
8/2/2019	Robert Smith	robert.smith@ucop.edu	Edited section 4 and fixed formatting in the Passphrase requirements table – 4.1 to make clear that the CISO can relax passphrase requirements when MFA is implemented. Minor corrections of typos and formatting.
8/21/2019	Robert Smith	robert.smith@ucop.edu	Updated to conform to standard style sheet.
10/3/2019	Robert Smith	robert.smith@ucop.edu	Approved by ITLC.
12/8/2022	Robert Smith	robert.smith@ucop.edu	Comprehensive update to reflect current state of technology, widespread use of MFA, Workgroup review, community input and review, streamlining of requirements, and feedback. Switched emphasis from passphrases to MFA. Approved by ITLC (Van Williams).

Contents

1 Purpose

Account management and authentication mechanisms are the primary method for protecting UC's Institutional Information and IT Resources and establishing access control. This Standard defines minimum requirements for account, passphrase, and authentication management.

This Standard is used in conjunction with Business and Finance Bulletin IS-3 – Electronic Information Security and its referenced Standards. The Event Logging Standard (4.3 Event Sources) and the IT Policy Glossary are helpful. See the Resources section for more information.

2 Scope

This Standard applies to methods used at or on behalf of UC to grant and manage access to Institutional Information or IT Resources.

Some technology may have limitations that impact the feasibility of applying this Standard. In those cases, use either the IS-3 risk assessment process or the IS-3 exception process to appropriately manage cyber risk.

3 Definitions and Key Terms

- **Account Types:** The type and use of an account determine its authentication requirements. To distinguish between requirements based on account type, this Standard refers to several distinct kinds of accounts according to the following definitions. It is important to note that some accounts fall into more than one category (e.g., privileged user accounts and privileged functional accounts).
  - **User accounts** are those under the control of a specific individual and not accessible to others. They are frequently used to access multiple systems. They may be a single system, application-specific, or used across systems through a central authentication mechanism (e.g., Kerberos, AD, or SSO). This type of account may also be used in development, test, or production environments. Workforce Members may have more than one user account.
  - **Functional accounts** (sometimes called shared accounts) allow multiple individuals to appear as a single business entity or accomplish a single shared function (e.g., "physics department," "chancellor's office," "AppTest1," "DBTest1," "TestUser1," "TestRole1," "VendorABC1," "SupplierXYZ4," etc.).
  - **Service accounts** are intended for automated processes such as running batch jobs or applications. Service accounts must have a strictly defined scope of access.
  - **Privileged accounts** are used to configure or significantly change the behavior of a computing system, device, application, or other aspects of the IT Resource or IT infrastructure. Privileged accounts include, but are not limited to, UNIX "root" accounts, Windows Administrator accounts, and device configuration accounts. Privileged accounts must have a strictly defined scope of access.
- **Emergency use** refers to access to Institutional Information or IT Resources that are not accessible using normal or routine controls. An emergency use account provides immediate access to an IT Resource using an account that may not normally be authorized for access.

- **Multifactor Authentication (MFA)** is an authentication system that requires more than one distinct authentication factor for successful authentication. Examples include a biometric identifier such as a fingerprint, iris scan, or voiceprint, or a certificate, security token, or other confirmation of identity presented to verify that access to a resource is allowed. MFA can be performed using a multifactor authenticator or a combination of authenticators that provide distinct factors.
- **Passphrase** is a sequence of words or other text used as part of the authentication process. A passphrase is similar to a password in usage but is longer for added security.

Note: The term "passphrase" is the preferred term. The legacy term "password" is phased out in this version of the Standard. Where implementations use the legacy term, the passphrase requirements still apply.

- **Personal Identification Number (PIN):** A user-memorized secret typically consisting of numerical digits.

For more information about definitions, consult the IT Policy Glossary.

4 Account and Passphrase Management

This section applies to accounts and the associated passphrase or other factors used to access Institutional Information or IT Resources. This includes accounts for Workforce Members and other users.

4.1 Passphrase and PIN strength

4.1.1 The CISO must approve the passphrase requirements when MFA is enforced for access to Institutional Information or IT Resources.

4.1.2 When MFA is not enforced for access to Institutional Information or IT Resources or is enforced for only some use cases, Workforce Members must ensure that the passphrase minimum complexity is based on passphrase length as follow:

- A CISO-approved passphrase strength meter, or;
- 8-11 characters: mixed case letters, numbers, and symbols.
- 12-15 characters: mixed case letters and numbers.
- 16-19 characters: mixed case letters.
- 20 or more characters: no composition restrictions.

4.1.3 Workforce Members accessing IT Resources over a network containing Institutional Information classified at P3, P4, A3, or A4 must verify that when the passphrases are created or updated, they are not commonly used, expected, or compromised.

4.1.4 Workforce Members must ensure that PINs are at least six (6) characters in length.

4.2 Passphrase reuse

4.2.1 Workforce Members must not reuse passphrases.

4.2.2 Workforce Members must not use UC passphrases for non-UC social media, personal shopping, or other non-UC purposes.

4.2.3 Workforce Members must not use personal passphrases used on non-UC services or accounts for UC-related services or accounts.

4.3 MFA

4.3.1 Workforce Members accessing IT Resources containing Institutional Information classified at P3, P4, A3, or A4 over a network must use MFA.

Note: MFA is highly recommended but does not apply as a requirement when a Workforce Member, patient, student, or other person is exclusively accessing their information for personal purposes.

Note: The MFA requirement can be replaced with compensating controls when operating inside a formally secured and managed environment (e.g., using the medical records system to provide care to a patient in an access-controlled treatment room). These use cases must be documented in the risk assessment and communicated to users of the system(s). See the implementation Frequently Asked Questions (FAQs) for more information.

4.4 When to change passphrases

4.4.1 For user or functional accounts where MFA is not enforced to access Institutional Information or IT Resources classified at P3, P4, A3 or A4, Workforce Members must ensure passphrases are changed on a regular basis.

- The Risk Assessment or Risk Treatment Plan will determine the frequency of required passphrase changes and related mitigation.
- In the absence of a specific determination on change frequency, the frequency must be six (6) months or less.

4.4.2 Workforce Members must immediately change their passphrase(s) if:

- The passphrase is independently discovered.
- There is an unauthorized disclosure of the plaintext and/or hashed passphrases.
- A suspected compromise has occurred.
- A device has been lost or stolen that may contain passphrases.

4.5 Restrictions on sharing passphrases, PINs, and authentication devices/tokens

4.5.1 Workforce Members must not share user account passphrases, PINs, devices used to authenticate the user (e.g., mobile phones), or tokens (e.g., multifactor tokens, smartcards, etc.) with others unless otherwise allowed in this Standard.

4.5.2 Units, Service Providers, Workforce Members, and Workforce Managers must not request or require a Workforce Member or user to share the passphrase to a user account (e.g., as a condition of employment or to provide technical support to access IT Resources, etc.).

4.5.3 Workforce Members must report the following via the security office or an approved Location or Unit-reporting mechanism:

- Compromised passphrases or PINs.
- Unauthorized disclosures of passphrases or PINs.
- Unauthorized use or loss of authentication devices or tokens.

4.5.4 Workforce Members must not use UC passphrases or any other UC authentication secret for non-UC social media, personal shopping, or other non-UC applications.

4.6 Storage of passphrases

4.6.1 Workforce Members storing passphrases for Wi-Fi and other applications on portable single-user devices (e.g., mobile phones, tablets, laptops, etc.) must use a compliant PIN or passphrase to access the device and enable encryption.

4.6.2 Workforce Members must ensure passphrases, PINs, and other authentication secrets (e.g., codes, bypass codes, private keys, etc.) are encrypted using a CISO-approved method when electronically stored (i.e., not stored in plaintext).

4.6.3 Location CISOs may approve using passphrase managers or other software applications (e.g., Privileged Access Manager, Keychains, etc.) designed to manage user passphrases and secrets securely.

4.6.4 Workforce Members accessing Institutional Information classified at P3 or P4 or IT Resources classified at A3 or A4 must not use the "remember your password" option in browsers or applications.

4.7 Initial passphrase, authentication secrets, and account provisioning and resets

4.7.1 Workforce Members initially provisioning accounts or MFA must use the CISO-approved method(s).

4.7.2 When a Workforce Member creates, takes control of, or resets the passphrase on behalf of another person with a single-user account, the IT Resource must require the user to create a new passphrase that complies with this Standard at the next use or login.

4.7.3 In cases when the preceding requirement is not technically possible, Workforce Members must ensure that these passphrases and authentication secrets are:

- Unique, not easily guessed, and comply with the passphrase complexity requirements of this Standard.
- Valid for 24 hours or less.
- Not reused.
- Communicated in compliance with Section 4.8.

4.8 Secure communication of passphrases and other authentication secrets

4.8.1 When communicating passphrases, temporary, or one-time secrets (e.g., passphrases, links, or code codes), or other authentication secrets (e.g., communicating a shared account passphrase, provisioning a new account or IT Resource, etc.), Workforce Members must:

- Use a secure communication method approved by the CISO.
- Not send passphrases or other authentication secrets (e.g., private or secret keys, bypass codes, etc.) in plaintext using email or with the file that the passphrase or secret protects.

4.9 User accounts for non-Workforce Members and guests

4.9.1 Workforce Members who provision accounts must ensure all non-Workforce Member user accounts (i.e., user accounts for those who are not Workforce Members) and guest

accounts with access to Institutional Information or IT Resources classified at P3 or P4 comply with this Standard.

4.9.2 CISOs must approve procedures for creating and managing non-workforce affiliate accounts provisioned through the Location's central identity and access management mechanism(s).

4.10 Use of functional accounts

4.10.1 Workforce Members must use functional accounts only for their intended business function.

4.10.2 For functional accounts with a shared passphrase, the shared passphrase must be:

- Stored securely.
- Changed when anyone with access to the passphrase leaves or separates (e.g., Workforce Member, Supplier, guest, or a third party).
- Changed based on the risk of discovery over time.

4.10.3 Functional accounts used to access Institutional Information or IT Resources classified at P3, P4, A3, or A4 must use auditable features (e.g., impersonation, sudo, delegation, privilege access manager, tracking ticket/record, etc.).

Note: Accounts used to authenticate automatically or anonymously (e.g., "kiosk1," "guest1", etc.) are treated as functional accounts for this Standard.

4.11 Use of service accounts

4.11.1 UISLs must ensure service accounts have a strictly defined scope and cannot be used for other purposes.

4.11.2 Workforce Members must ensure that service accounts used to access Institutional Information classified at P3 or P4 and IT Resources classified at A3 or A4 are disabled from interactive login or screen/user interface sessions.

4.11.3 Workforce Members must ensure that service accounts used to access IT Resources classified at A3 or A4 are accessible to more than one authorized Workforce Member.

4.11.4 Workforce Members creating service accounts must ensure they are distinguishable from Workforce or other account types.

4.11.5 Workforce Members who manage passphrases for service accounts must:

- Store the passphrase securely as outlined in this Standard.
- Access the passphrase in a controlled and auditable manner.

4.12 Emergency use of shared service account passphrases and credentials

4.12.1 In the event of an emergency and/or if the designated and authorized user (e.g., super-passphrase holder) is unavailable, UISLs must ensure that an auditable process is established or identified to maintain custody of service account shared authentication secrets used to access Institutional Information or IT Resources classified at A3 or A4.

4.12.2 UISLs must ensure the emergency use process:

- Protects authentication secrets and as needed, the process.
- Ensures that shared authentication secrets are changed after emergency use.
- Delineates how these secrets are logically or physically accessed.
- Identifies who becomes responsible for access to and/or reset of the secrets after emergency use.

- Allows for the auditing or review of the shared authentication secrets.
- Tests the access to and reviews the use of these accounts.
- Limits emergency access to the minimum data and functionality needed to perform the task.

4.13 Privileged accounts and privilege grants for installation and maintenance

4.13.1 UISLs must ensure that an auditable process is established or identified that:

- Manages privileged access needed to perform installations, updates, or other administrative activities.
- Enables these accounts to perform the specific administrative task(s) required.
- Disables the privileged access when the specific administrative task(s) are complete.
- Ensures privileged accounts have a strictly defined scope and cannot be used for day-to-day tasks (e.g., email, web browsing, messaging, web meetings, etc.).
- Considers the risk of lateral movement if compromised.
- Ensures privileged access is promptly reduced or removed when it is no longer needed for UC business purposes.

4.13.2 Privileged accounts used to access Institutional Information or IT Resources classified at P3, P4, A3, or A4 must use auditable features (e.g., impersonation, sudo, delegation, privilege access manager, tracking ticket/record, etc.).

4.14 Inactive accounts

4.14.1 Workforce Members must ensure accounts under their control or area of responsibility that have not been accessed for one hundred and eighty (180) consecutive days are reviewed. If accounts are not needed, then they must be disabled or removed.

4.14.2 CISOs may approve longer no-access periods.

4.14.3 CISOs may approve services or login capability to retirees, emeritus faculty, or staff for sabbaticals, leaves or other planned absences, and other use cases.

4.15 Account management process

4.15.1 UISLs must ensure that a process or procedure is in place that identifies, manages, reviews, decommissions, and renews the use of functional, service, privileged, and non-Workforce accounts managed by the Unit. The process or procedures must:

- Record who has access (e.g., guest, Workforce Member, Supplier, etc.) to what account.
- Record the purpose of the account.
- Record use cases involving the use of the account.
- Record the applications, services, and IT Resources that depend on the account.
- Ensure that each functional, service, privileged, and non-Workforce account has a designated proprietor who is responsible and accountable for following the process.
- Ensure that emergency use methods or accounts have a designated proprietor who is responsible and accountable for following the process.
- Be documented and accessible to responsible Workforce Members.

- Be reviewable or auditable.

4.16 Access rights adjustments

4.16.1 UISLs must ensure that a process is in place for all account types to update or adjust access rights when changes occur [e.g., job responsibilities, termination, access is no longer required, IT Resource (service) retired, etc.] or the account is no longer needed. The timeline for access right adjustments is:

- Within five (5) days for Institutional Information or IT Resources classified at P3, P4, A3, or A4.
- Within thirty (30) days for Institutional Information or IT Resources classified at P1, P2, A1, or A2.

5 Authentication Management

This section focuses on how Workforce Members implement authentication management related to Institutional Information and IT Resources. The process that provides credentials or other authentication secrets to authorize access to Institutional Information, IT Resources, or an operation/role in a system must manage cyber security risks.

5.1 MFA configuration

5.1.1 Workforce Members implementing IT Resources must ensure that the MFA configuration for user, functional, or privileged accounts that access Institutional Information or IT Resources classified at P3, P4, A3 or A4:

- Presents the user with an MFA challenge using a CISO-approved system and uses the Location-approved authentication system; or
- Implements compensating controls approved through the risk assessment.

5.1.2 Workforce Members implementing IT Resources must ensure user, functional, or privileged accounts used to access Institutional Information or IT Resources classified at P4 or A4 are subject to an MFA policy that permits remembered browsers/devices for no longer than eighteen (18) hours or the CISO-approved duration.

5.2 IT Resource account configuration

5.2.1 Workforce Members implementing IT Resources must do the following:

- Configure IT Resources with separate accounts or roles for privileged (administrator) and unprivileged (user) access.
- Grant privileged access through an escalation mechanism that identifies which user was granted the additional privileges.
- Grant/use privileged access only for as long as necessary to complete the task that requires the additional privileges.
- Ensure that when privilege escalation is not feasible and privileged account passphrases must be shared with multiple individuals (e.g., network appliance, switch, or router passphrases), the sharing is justified and approved following the exception process in IS-3, III, Section 2, 2.2.
- Ensure that each identification or authentication token is unique to the person and requesting device.

5.3 User account and reset lockout

5.3.1 The responsible Workforce Member must configure the IT Resource login features to do one or more of the following in response to ten (10) or more failed user passphrase login or user security question response attempts:

- Lock the account to prevent additional attempts.
- Delay the next attempt progressively (rate limiting).
- Present a challenge such as a CAPTCHA.
- Require an out-of-band authorization code.
- Use other risk-based or adaptive authentication techniques to identify whether user behavior falls within typical norms.

5.4 Recovery of passphrases and authenticators using security questions or other methods

5.4.1 Workforce Members implementing or managing security challenge questions (e.g., selecting, acquiring, or designing) to reset passphrases must:

- Enroll users with at least three (3) questions.
- As a means of authentication, avoid knowledge-based challenge questions (e.g., where, when, and what questions) whose answers are likely to be available from public sources (e.g., birthday, address, prior address, school attendance, prior employment, graduation data, etc.).
- Ensure that questions are not predictable; the user should be challenged with random questions from the set of available questions.
- Review the security questions with the CISO and address identified risks resulting from the review.

5.4.2 Workforce Members implementing or managing other recovery methods (not question-based) for authenticator or passphrase recovery must review the recovery method with the CISO and address identified risks resulting from the review.

5.5 Integrated voice response systems (IVR) PIN or passphrase lockout (authentication)

5.5.1 Workforce Members must configure IVR systems to close the session after no more than five (5) failed attempts to enter the PIN.

5.6 Authentication services and passphrase management

5.6.1 Workforce Members must ensure IT Resources used for UC operations or to support UC operations and business processes use the Location-approved authentication method(s).

5.6.2 Workforce Members must ensure that IT Resources rely on CISO-approved Location or cloud authentication services and do not directly handle, store, or manage user account credentials.

- Technical feasibility issues must be addressed in the risk assessment or an approved exception.

5.6.3 Workforce Members implementing Location-wide authentication systems or Location-wide MFA must ensure that:

- The authentication system or MFA system is not susceptible to replay or authentication secret reuse attacks.

- When used to access Institutional Information or IT Resources classified at P3 or P4, MFA systems cannot be bypassed by any users, including administrative users, unless specifically documented and authorized through the risk assessment process[1].
- Before access is granted, all the authentication factors are successful.
- The duration of the authentication session is CISO-approved (e.g., SSO, MFA, etc.).
- Adoption of the approved bypass process for outage-related use cases (see 5.7.1).

5.6.4 Workforce Members implementing authentication systems using an approved exception that allows IT Resources to inspect plaintext credentials (e.g., prompting for a passphrase on a login form) directly must ensure that:

- The plaintext information accessible to the IT Resource is only for the minimum time necessary to complete the authentication process and is not stored anywhere.
- The plaintext information is securely deleted (including from application memory) once it is no longer needed.
- Any storage or caching is for the shortest duration possible.
- Any storage on electronic media (physical or virtual) uses a CISO-approved encryption method.

5.6.5 Unit Heads must adopt a CISO-approved method for cross-Location authentication and federated identity and access management.[2]

5.6.6 Passphrases, PINs, and account recovery questions and related answers must be encrypted when stored.

5.6.7 Application secrets (e.g., database credentials, API keys, etc.) must be protected according to the controls identified in the risk assessment.

5.7 Approving bypass process for outage-related use cases

5.7.1 The CISO must approve the Location-wide access process for outage-related use cases (e.g., MFA down, authentication services down, etc.) when used to access Institutional Information or IT Resources classified at P3, P4, A3, or A4.

5.8 Identity assurance level

5.8.1 The CISO must approve a Location-wide identity assurance process to verify that user credentials are issued to the intended Workforce Member or affiliate. The process must:

- Be documented.
- Manage identity assurance risks.
- Manage records that link an individual with their login identification (e.g., username) information.
- Indicate how Units maintaining credential provider services comply.

---

[1] For payment card systems, the PCI DSS adds a limitation on administrative access without MFA that allows approved exceptions for a limited time only.

[2] The current approach is based on Simple Authentication Markup Language (SAML) 2.0. Contact the Location Security Office for implementation details.

5.8.2 UISLs must ensure that the Unit follows the identity assurance process approved by the CISO.

6 References

UC Policy

Business and Finance Bulletin IS-3 – Electronic Information Security

Encryption Key and Certificate Management Standard

Event Logging Standard

External References

NIST Special Publications 800-63-3 - Digital Identity Guidelines

ISO 27002:2013 - Section Cross Reference

9.0 Access control

9.2.1 User accounts

9.2.3 Management of privileged access rights

9.2.4 Management of secret authentication information of users

9.2.5 Review of user access rights

9.2.6 Removal or adjustment of access rights

9.3 User responsibilities

9.3.1 Use of secret authentication information

9.4 System and application access control

9.4.1 Information access restriction

9.4.2 Secure login procedures

9.4.3 Password management systems

9.4.4 Use of service accounts and privileged utility programs

7 Frequently Asked Questions (FAQs)

1. **Question**: Can the CISO delegate responsibilities that are assigned in this standard?

Answer: Yes. Other Workforce Members should know who the delegate is, and that person should have the authority to manage cyber risk. The responsibilities must be clear, known by others, and provide accountability for actions.

For example, a Workforce Manager responsible for identity and access management might be assigned responsibilities to establish, monitor, and adjust passphrase complexity requirements, and others should know who that person is.

2. **Question**: What is the goal of the CISO approving a procedure for accounts and passphrases for affiliates?

Answer: The goal is to make sure that any third party (non-Workforce) accounts that access IT Resources or Institutional Information have a process that adequately manages risk. The procedure should make sure no permission can be leaked to an unauthorized or uninvited affiliate and that the access control configurations and processes will not result in unintended or unauthorized access.