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.
10/3/19	Robert Smith	robert.smith@ucop.edu	Approved by ITLC.

Contents

1 Background and Purpose

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

Following the requirements in this Standard ensures good security practices that help minimize cyber risk. IT Workforce Members and Unit Information Security Leads (UISLs) should consult this Standard and NIST 800-63-3, particularly when upgrading systems or renewing agreements. NIST 800-63-3 provides forward-looking guidance on topics covered in this Standard.

Those designing and implementing new systems and processes or making major upgrades should meet the requirements in NIST 800-63-3 Authenticator Assurance Level AAL2 and Identity Assurance Level IAL2. With these processes and technologies in place, NIST 800-63-3 guidance is an approved alternative to this Standard.

2 Scope

This Standard applies to all accounts, passwords and other authentication methods used at or on behalf of UC to access Institutional Information or IT Resources.

3 Definitions and Key Terms

- **Account Types:** The type and usage of an account generally determines its authentication requirements. In order to distinguish between requirements based on account type, this Standard refers to several different 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, privileged functional accounts).
  - **User accounts** are those under the control of a specific individual and are not accessible to others. They are frequently used to access multiple systems. They may be system/application specific or used across systems through a central authentication mechanism (e.g., Kerberos, AD, SSO). This type of account may also be used in development, test or production. Workforce Members may have more than one user account.
  - **Functional accounts** (sometimes called shared accounts) can be accessed by multiple individuals to allow them to appear as a single business entity or accomplish a single shared function (e.g., "physics department" or "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 aspect 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.

- **Hash (Hash Function)**: A value computed from a cryptographic function that maps a string of characters of arbitrary length (passphrase + salt) to a fixed-length bit string (the hash value).
- **Multifactor Authentication (MFA)**: An authentication system that requires more than one distinct authentication factor for successful authentication, (e.g., 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). Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors.
- **Passphrase**: 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 generally longer for added security.
- **Password**: A string of characters (letters, numbers and/or symbols) used to authenticate an identity, verify access authorization or derive cryptographic keys. Generally composed of not more than 8-16 characters. A type of memorized secret. A type of authenticator comprised of a string of characters intended to be memorized or memorable by the user, permitting the user to demonstrate something they know as part of an authentication process.

Note: The terms "password" and "passphrase" can be used interchangeably. "Passphrase" is often used to encourage stronger security. This document generally uses "passphrase." "Password" is used only to improve understanding, usually due to historical convention.

- **Personal Identification Number (PIN):** A memorized secret typically consisting of numerical digits.
- **Salt**: A non-secret, random value that is used as an input to passphrase hashing in order to make discovery of a passphrase harder (e.g., a random set of characters added to a passphrase prior to hashing it to make it harder for an attacker to learn the passphrase).

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 factor used to gain access to Institutional Information and IT Resources. This includes accounts for Workforce Members and other users.

At the time of issuance of this Standard, there are two important shifts underway in how users login (authenticate their access) to systems.

The first and most important is the shift to multifactor authentication (MFA). When a Location adopts MFA, the CISO may relax or eliminate the passphrase complexity requirements and passphrase change requirements. Note that some external requirements may still impose limitations (e.g., PCI-DSS).

The second shift is the move from short passwords to long passphrases. When long passphrases are consistently supported, complexity requirements are eliminated.

4.1 Passphrase, password and PIN strength

Include:	Avoid:
● Eight (8) characters or more when possible following this sliding scale: ▪ 8-11 characters: mixed case letters, numbers and symbols. ▪ 12-15 characters: mixed case letters and numbers. ▪ 16-19 characters: mixed case letters. ▪ 20+ characters: no restrictions. ● Based on the sliding scale above, choose characters from three or more of the following character classes, particularly if the IT Resource or system prohibits long passphrases: ▪ Alphabetic lower case (a-z). ▪ Alphabetic upper case (A-Z). ▪ Numeric (0-9). ▪ Punctuation and other characters (e.g., !@#$%^&*()_+|~-=\`{}[]:";'<>?,./). (When permitted by the technology 'space').	● A derivative of the username. ● A single dictionary word (forwards or backwards) preceded and/or followed by any other single character (e.g., secret1, 1secret, secret?, secret!). ● A passphrase used in the past (at UC or elsewhere). ● Obvious substitutions in common words (123Longp@ssw0rd, 1 l0v3 MY c@T!). ● Easy-to-guess words and phrases such as names of family members, pets, friends or coworkers; computer terms and names; commands; sites; companies; hardware; software; movie themes; sports teams; celebrities. ● Personal information, such as addresses, birthdays or phone numbers. ● Easy word, keyboard or number patterns such as aaabbbcccd, qwerty, zxcvbnm, 1234567890, 12345,123321, 09876, etc. ● Simple changes forming a fixed pattern, even to a good passphrase (e.g., MyGoatt6244!Q12017, MyGoatt6244!Q22017, MyGoatt6244!Q32017 or 981WegFdnN*!-1, 981WegFdnN*!-2, 981WegFdnN*!-3). See Appendix A for more examples of passphrases to avoid.
● PINs must be at least six (6) characters in length.	● Four-digit PINs. ● Easy-to-guess patterns in PINs (e.g., 0000, 1111, 1234, 12345, 54321, 4321, etc.). ● Easy-to-guess PINs with personal information (e.g., phone numbers, birthdays, etc.).

4.2 Multifactor authentication

Accounts used to access Institutional Information or IT Resources classified at Protection Level 3 or higher and IT Resources classified at Availability Level 3 or higher must use multifactor authentication.

Note: Multifactor authentication does not apply as a requirement when a Workforce Member, patient, student or other person is exclusively accessing their own information for personal purposes.

Note: The multifactor authentication 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).

4.3 When to change passphrases

For accounts without multifactor authentication that are used to access Institutional Information classified at Protection Level 4, IT Resources classified at Protection Level 4 or IT Resources classified at Availability Level 3 or higher, Workforce Members must change user account passphrases on a regular basis. The Risk Assessment, Risk Treatment Plan or CISO will determine the frequency of required passphrase changes. In the absence of specific determination, if multifactor authentication is not in place, use a frequency of six (6) months or less.

Workforce Members must change their passphrase immediately if it is independently discovered, if it is publicly disclosed, if a suspected compromise has occurred or if their device has been lost or stolen. This includes discovery of plaintext and/or hashed passwords or passphrases.

Contracts, regulatory requirements and compliance requirements may impose specific controls on accounts and authentication. In all cases, Workforce Members must follow the strongest requirements.

4.4 Sharing passphrases, PINs, authentication devices/tokens and no request for passphrases

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.

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

Workforce Members must report any compromise or unauthorized disclosure, use or compromise of any passphrase or other authentication device to the UISL or CISO (e.g., via the security office or a Location reporting mechanism).

4.5 Using UC usernames and passphrases for non-UC business

Workforce Members must not use UC user account names (email, logon name or netid) as the primary identifier on non-UC accounts created for non-UC purposes (e.g., username@UCcampus.edu must not be used as the account name for a personal account).

Workforce Members must not use UC passphrases for social media, shopping or other personal applications.

Note: Many Locations provide UC email accounts to retirees, emeritus faculty/staff and others. These accounts are not subject to the reuse of user name restriction when intended to be general purpose user email accounts.

4.6 Storage of user passphrases

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

Location CISOs may approve the use of password managers or software applications designed to manage user passwords and passphrases securely.

Workforce Members accessing Institution Information classified at Protection Level 3 or higher or IT Resources classified at Availability Level 3 or higher must not use the "remember your password" option in browsers or user/general applications.

Passphrases and PINs must be encrypted when stored electronically.

4.7 Secure communications of passphrases

When communication of passphrases is required (e.g., communication of a shared account passphrase) Workforce Members must:

- Use a secure communication channel.
- Not send passphrases or other secrets in plain text using email or with the file the passphrase protects. Temporary or onetime passwords may be communicated using SMS, email, an out-of-band authorization code or during a phone call (but not via voicemail).

4.8 Initial passphrase or secrets

When a Workforce Member creates, takes control of or resets the passphrase for an account, the IT Resource must require the user to create a passphrase that complies with this Standard.

In cases when the preceding requirement is not technically possible, the initial passphrase must be unique, must comply with the passphrase complexity requirements of this Standard and must be communicated securely.

IT Workforce Members must:

- Set a short time limit of 24 hours or less on the life of links or codes providing temporary access, and they must not reuse them.
- Make sure temporary passphrases or access codes are unique and not easily guessed.

4.9 Use of named functional accounts

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

Functional accounts must not be used to access any Institutional Information or IT Resources classified at Protection Level 4 and/or Availability Level 4.

The passphrase for the functional accounts must be:

- Stored securely.
- Controlled and auditable.
- Changed when anyone with access to the account leaves or separates (e.g., Workforce Member, Supplier, guest or other third party).
- Changed frequently based on risk of discovery (e.g., autologin systems).

UISLs must record all applications and IT Resources that use the functional account.

Functional accounts must be disabled when not in use.

Functional accounts must have a limited lifetime and be periodically renewed based on risk.

Note: The purpose of a named or shared functional account is often to support specified, routine business functions that do not require elevated access privileges. Sharing an account through auditable features such as impersonation, sudo and delegation is permitted. These methods must be used rather than passphrase sharing whenever possible.

Note: Auto logon systems that automatically log users (e.g., kiosk1, guest1, etc.) should be treated as functional accounts.

4.10 Use of service accounts

IT Workforce Members must ensure that service accounts used to access Institutional Information classified at Protection Level 3 or higher and IT Resources classified at Availability Level 3 are disabled from interactive login or screen/user interface sessions when possible.

Service accounts essential to the operation of an IT Resource (e.g., system or application) must be accessible to more than one authorized Workforce Member.

Service accounts must have a limited lifetime and be periodically renewed based on risk.

Workforce Members handling passphrases for service accounts must:

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

Note: Access by more than one authorized person does not apply to a single-user system or an application that is not used for a production process that supports a Unit's function.

4.11 Management of service accounts or functional accounts

Each service or functional account must have a designated owner who is responsible and accountable for the management and appropriate protection of account credentials and access.

The service or functional account owner must document:

- A list of all individuals who have access to the account.
- The purpose of the account.
- All use cases involving use of the shared or functional account.
- The services and applications that depend on the account.

4.12 Privileged Accounts for installation and maintenance

Units must document and approve privileged access accounts needed to perform installations, updates or other administrative activities, and, if possible, only enable them to perform the specific administrative task(s) and then disable them.

UISLs must ensure privileged accounts have a strictly defined scope of access and cannot be used for day-to-day tasks (e.g., email, web browsing, messaging, web meetings, etc.).

When privileged access is no longer needed for UC business purposes, UISLs must appropriately and promptly reduce or remove access.

4.13 User accounts for non-Workforce Members and guests

All non-Workforce Member user accounts (user accounts for those who are not Workforce Members) and guest accounts with access to UC Institutional Information classified at Protection Level 2 or higher must comply with this Standard.

Procedures for accounts and passphrases for affiliates must be set by the CISO at the Location that is using/sponsoring the affiliate.

Accounts and passphrases used by parents, guardians and benefactors of students for purposes of paying fees, expenses or similar functions must be in compliance with this Standard.

4.14 Account maintenance: removing unneeded accounts and/or access rights

When access to Institutional Information or an IT Resource is no longer needed for UC business purposes, UISLs must disable or remove the access rights.

When access to all Institutional Information and IT Resources is no longer needed, the UISL must disable or remove the user account.

Workforce Member accounts must be deleted, disabled, have their access rights restricted or have their access rights removed from any IT Resource for which they no longer need access at the end of the Workforce Member's employment, at the time of a change of job responsibilities or during an approved leave of absence.

Rights must be removed on this schedule:

- For Institutional Information or IT Resources classified at Protection Level 3 or higher and/or Availability Level 3 or higher, five (5) days or less.
- For Institutional Information or IT Resources classified at Protection Level 1 or 2 and/or Availability Level 1 or 2, thirty (30) days or less.

4.15 Inactive accounts

Accounts that have not been accessed for 180 consecutive days must be reviewed. If not needed, they must be disabled or removed.

CISOs may approve longer no-access periods for sabbaticals, leaves or other planned absences.

Note: Locations may offer some services or login capability to retirees, emeritus faculty/staff or similar approved users, with a longer, CISO-approved expiration deadline.

4.16 Emergency use of shared service account passphrases and credentials

Units must have proper auditable procedures in place to maintain custody of service account "shared secrets" in the event of an emergency and/or if the super-passphrase holder is unavailable.

UISLs must ensure that shared secrets are changed after emergency use.

These documented procedures must:

- Be appropriately secured.
- Delineate how these passphrases are logically or physically accessed.
- Identify who becomes responsible for access to and/or reset of the passphrase after emergency use.
- Audit the use of these shared secrets.
- Test the access to and audit the use of these accounts.
- Limit emergency access to the minimum data and functionality needed to perform the task.
- Establish account naming or recognition (delineation) requirements.

5 Authentication Management

This section focuses on ensuring proper information security risk management related to authentication mechanisms. The process by which one provides credentials or other secrets in order to authorize access to Institutional Information, IT Resources or an operation/role in a system must be secure.

5.1 IT Resource account configuration

IT Workforce Members must:

- Configure IT Resources (devices) with separate accounts 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.

When use of 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 must be justified and approved following the exception process in IS-3, III, Section 2, 2.2. The use, management and tracking of privileged account access must, at a minimum, meet the passphrase sharing requirements for service accounts as defined in Section 4.10.

5.2 Account and reset lockout

The IT Workforce Member responsible for an IT Resource must ensure the IT Resource or application is configured to do one or more of the following in response to ten (10) or more failed login or security question response attempts:

- Lock the account to prevent additional attempts.
- Progressively delay the next attempt (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.

5.3 Security questions

IT Workforce Members implementing or managing security challenge questions (e.g., selecting, acquiring or designing) must:

- Use at least three (3) questions.
- Avoid, as a means of authentication, 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 predicable and that each user is presented random questions from the set of available questions.
- UISLs implementing systems or applications using this feature must review the application with the CISO.

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

IT Workforce Members must configure IVR systems to close the session after five (5) failed attempts to enter the PIN.

5.5 Authentication services and passphrase management

Workforce Members who are application developers and/or IT Workforce Members must ensure applications used for UC operations or to support UC operations and business processes use the Location-approved authentication method(s).

IT Workforce Members and the applications they implement must not handle, store or manage user credentials directly, and must rely on Location-approved authentication services.

When an approved exception allows applications to directly inspect plaintext credentials (e.g., prompting for a passphrase on a login form), the plaintext information must:

- Be accessible to the application for the minimum time necessary to complete the authentication process and not be stored.
- Be securely deleted (including from application memory) once it is no longer needed.

5.6 Protecting authentication secrets

IT Workforce Members managing authentication secrets must:

- Never store them in clear text.
- Never store them in the same file or container as other secrets unless specifically approved by the CISO for that purpose.
- Use salts that are cryptographically sound and generated by a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) and at least 32 bytes (256 bits).
- Protect answers to security questions in the same way that they protect passphrases.

Note: See the Encryption Key and Certificate Management Standard for more information. See also the Enterprise Architecture group's Passphrase Storage Standard - EA Artifact Item EA-035.

6 References

UC Policy

Business and Finance Bulletin IS-3 – Electronic Information Security

External References

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

NIST Special Publication 800-63a - Digital Identity Guidelines

NIST Special Publication 800-63b - Digital Identity Guidelines

NIST Special Publication 800-63c - Digital Identity Guidelines

UC EA Standards

EA Artifact Item EA-035 – Password Storage

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 Appendix A – Password and Passphrase Guidance

Introduction

Individual passwords are often the weakest link in computer security. UC works to keep hackers out of your personal files and away from UC-only IT Resources (e.g., email, files containing personal information, licensed software), but easily guessed passwords can undermine the protective structures in place.

To address this problem, UC now recommends "passphrases" instead of passwords. Passphrases are longer but easier to remember than complex passwords. If well chosen, they can provide better protection against hackers.

Locations may require Workforce Members who work in UC Units that are subject to the security rule under Health Insurance Portability and Accountability Act (HIPAA) to change their passphrases more frequently based on the Location/Unit Risk Assessment.

Units that process credit cards are required to change passwords used in the Cardholder Data Environment (CDE) every 90 days.

Many Locations are using passphrase strength checkers to prevent the use of commonly used, weak or compromised passwords because hackers try these first.

Creating a passphrase

A passphrase is a series of words that can include spaces instead of a single password. Passphrases should be at least 16 to 25 characters in length (spaces count as characters). Longer is better because the increased length provides so many possible permutations that a standard password-cracking program cannot be effective. It is also always a good practice to disguise any simplistic features of a passphrase by throwing in elements of weirdness, nonsense or randomness.

<u>Examples of passphrases (do not use these):</u>

- eggs with crispy hydrants
- soothing and happy singing therapy

<u>How to improve your passphrase:</u>

- Punctuate and capitalize your phrase:
  - Eggs with crispY hYdrants!
  - soothinG and happY SinginG TherapY?
- Add in a few numbers or symbols from the top row of the keyboard and some deliberately misspelled words, and you will create an almost un-guessable key to your account:
  - Eggs w/22 Crispy Hydrants!
  - S00thing & Happy 5 Singing Therapy?
- Avoid passwords that were or might have been compromised.

Do not reuse passwords that you have used in the past, especially on sites like Yahoo!, LinkedIn, Adobe, eBay, AOL, Twitch, Tumblr, Facebook, Living Social, Anthem, other small websites or other services that might have been compromised.

Commonly used passwords that attackers will try first:

123456	abc 123
password	admin
12345	121212
12345678	flower
football	passw0rd
qwerty	dragon
1234567890	sunshine
1234567	master
princess	hottie
1234	loveme
login	zaq1zaq1
welcome	password1
solo	qwertyuiop
123321	987654321
66666666	77777777
654321	55555555
1q2w3e4r5t	google
123qwe	zxcvbnm
1q2w3e	changeme

Other weak password families to avoid:

- Sports, team names (with any numbers).
- Prominent sports figure names (with any numbers).
- Prominent bands, actors, artists, academics, astronomers, etc.
- Movie theme words.
- Movie and comic book characters.
- Movie theme phrases.
- Song lyrics.
- Birthdays.
- Addresses.
- Phone numbers.
- Anything an attacker might glean or guess from your social media posting or group memberships, job or role.