Weill Cornell Medicine

11.15

Password Policy

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued:
Last Updated: September 5, 2023
Last Reviewed: September 5, 2023

Contents

Weill Cornell Medicine

Policy Statement

All individuals are responsible for safeguarding their system access login (“CWID”) and password credentials and must comply with the password standards identified in this policy. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this policy.

Reason for Policy

Assigning unique individual logins and requiring password protection is one of several primary safeguards employed to restrict access to the Weill Cornell Medicine networks, systems, applications, and data. If a password is compromised, inappropriate access might be obtained by an unauthorized individual. Individuals with CWIDs are responsible for safeguarding against unauthorized access to their account, and as such, must conform to this policy in order to ensure passwords are kept confidential and designed to be complex and difficult to guess. The parameters in this policy are designed to comply with relevant legal and regulatory standards, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Entities Affected by this Policy

All units of Weill Cornell Medicine, including Weill Cornell Medicine-Qatar.

Who Should Read this Policy

All members of the Weill Cornell Medicine community utilizing Weill Cornell Medicine information technology resources. All stewards and custodians of Weill Cornell Medicine data.

Web Address of this Policy

https://its.weill.cornell.edu/policies/

Contacts

Direct any questions about this policy, 11.15 – Password Policy, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu

1. Individual Responsibilities

Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

a) Temporary or default passwords must be changed immediately upon first use. Initial passwords must be securely transmitted to the individual.

b) Unless otherwise provided for in this policy, passwords must never be shared with other individuals or organizations. A compromised or suspected compromised CWID password is a reportable ITS security incident.

c) Employees—including faculty, physicians, and supervisors—as well as students and other Weill Cornell Medicine members, should never ask anyone else for their password. If an individual is inappropriately asked to provide their password to another individual or sign into a system for someone else under their login, the individual is obligated to report this to the Privacy Office or ITS Security using one of the methods outlined below.

d) Passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats. Passwords may be stored in a secure password manager, such as LastPass, as long as the master password is kept private and meets the requirements in this policy.

e) Individuals must never leave themselves logged into an application or system where someone else can use their account.

   i. To access shared workstations (e.g., clinical exam rooms, kiosks), ITS will provide a limited-use shared account. Once logged in to the shared workstation with the shared account, individual credentials must then be used for accessing applications, such as Epic.

   ii. ITS will never ask for a password. In ITS support scenarios where an ITS account cannot be used, an individual may allow a technician to utilize their computer under the individual's account even if the individual is unable to be present during the entire support session. The individual should not share their password with the technician. All ITS support technicians are expected to abide by ITS policy 11.01 – Responsible Use of Information Technology Resources and their actions may be audited as needed.

   iii. In the event of a hardware malfunction and the device needs to be repaired by a third-party, the device owner should backup the data to a secure storage location and securely wipe the device before providing it to the third-party. ITS can assist with this and other related processes. Passwords should never be shared with third-party repair providers.

f) In the event that a password needs to be issued to a remote individual or third-party, the password must be sent with proper safeguards (e.g., shared via a secure password manager or sent via an encrypted email message).

g) Individuals with access to service accounts or test accounts must ensure the account password complies with this policy and keep the password stored in a secure password manager.

h) In the event a password breach or compromise is suspected or confirmed, the incident must be reported to ITS Security immediately using one of the methods outlined below.

2. Responsibilities of Systems Processing Passwords

All Weill Cornell Medicine systems—including, but not limited to, servers, applications, and websites that are hosted by or for Weill Cornell Medicine—must be designed to accept passwords and transmit them with proper safeguards.

- Passwords should be prohibited from being displayed when entered, although it is suitable to have a method to toggle visibility as needed.

- Passwords must never be stored in clear, readable format. Reasonably strong, brute-force resistant hashing methods or encryption must always be used. Hashing, including salting and peppering (if possible), should be used in lieu of encryption.
- Hashed or encrypted passwords must never be accessible to unauthorized individuals.
- Passwords must never be stored as part of a login script, program, or automated process.
- Where any of the above items are not supported, a variance request should be submitted to ITS for review pursuant to ITS policy 11.20 – Variances. Appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to passwords.

3. Password Requirements

The following parameters indicate the minimum requirements for passwords for all accounts (except for passcodes defined in *Service Accounts and Test Accounts* below):

- At least sixteen (16) characters;
- Unique and different from passwords used for other services (e.g., personal banking or email);
- Changed at the regularly scheduled time interval as defined in this policy or upon suspicion or confirmation of compromise;
- Not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, CWID, telephone numbers, dates of birth, etc.);
- Not reasonably vulnerable to a dictionary or brute-force attack (see *Recommendations for Creating Compliant Passwords* below);
- Not reused for at least six (6) generations; and,
- Significantly dissimilar to any previous passwords.

4. Password Expiration

Most individuals are no longer required to change their passwords at fixed intervals. Some account types, such as privileged accounts, must still adhere to regular password changes as defined below.

In all cases, ITS Security reserves the right to reset or expire an individual's password in the event a compromise is suspected, reported, or confirmed. This helps prevent an attacker from making use of a password that may have been discovered or otherwise disclosed.

4.01 Standard Accounts

Standard accounts consist of members of the Weill Cornell Medicine community who are not system, application, or network administrators, privileged accounts, service accounts, or test accounts.

- All passwords must comply with the criteria above.

4.02 Privileged Accounts

Privileged accounts consist of individuals with elevated access to administer systems, applications, and network devices. Such individuals have administrator access that are more valuable targets for threat actors and consequently have a higher risk for compromise.

- Privileged account domain account passwords (e.g., Domain Administrators) must only be stored in the Privileged Access Management (PAM) system, and passwords must be rotated upon each use.

- Privileged accounts that cannot be stored in the PAM system must have their passwords changed every ninety (90) days.
- All passwords must otherwise comply with the criteria above.

4.03 Service Accounts and Test Accounts

Service accounts are accounts used by a system, task, process, or integration for a specific purpose. Test accounts are accounts used on a temporary basis to imitate a role, person, or training session. Passwords for service accounts and test accounts must be securely generated in accordance with this policy, distributed securely to the account owner, and stored securely in a password manager.

- Passwords must be changed when someone with knowledge of or access to the password leaves the institution or transfers into a new role.
- All passwords must otherwise comply with the criteria above.

5. Account Lockout

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all systems. Account lockout thresholds and durations vary based on the type of account, as defined below.

5.01 Standard Accounts

Standard accounts have the following lockout policy:

- Accounts will lockout after eighteen (18) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of fifteen (15) minutes, unless the ITS Service Desk is contacted and the individual's identity is verified in order for the account to be unlocked sooner.

5.02 Privileged Accounts

Privileged accounts have the following lockout policy:

- Accounts will lockout after twelve (12) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of fifteen (15) minutes, unless the ITS Service Desk is contacted and the individual's identity is verified in order for the account to be unlocked sooner.

5.03 Payment Card Industry (PCI) Accounts

Individuals responsible for processing payments in Weill Cornell Medicine's financial systems, such as Epic, must adhere to the Payment Card Industry's (PCI) Data Security Standard for account lockout:

- Accounts will lockout after ten (10) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of thirty (30) minutes, unless the ITS Service Desk is contacted and the individual's identity is verified in order for the account to be unlocked sooner.

5.04 Service Accounts and Test Accounts

Service and Test accounts have the following lockout policy::

- Accounts will lockout after twelve (12) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of fifteen (15) minutes, unless the ITS Service Desk is contacted and the individual's identity is verified in order for the account to be unlocked sooner.

6. Mobile Devices

Mobile devices accessing or storing Weill Cornell Medicine data, such as smartphones and tablets, shall be registered with ITS and managed by the mobile device management (MDM) platform. The following minimum passcode policy is in effect for all mobile devices:

- At least six (6) numeric digits;
- No repeating or sequential digits (e.g., 111111, 123456, or 101010); and,
- The passcode may not be one of three previously used passcodes.

Biometric authentication (e.g., facial or fingerprint recognition) on mobile devices may be used to unlock the device, but a compliant passcode must still be established.

If a password is used in lieu of a passcode, the password must be at least 6 characters.

Pattern unlocks or other authentication methods are not permitted.

A mobile device must be configured to wipe/erase itself after ten (10) invalid passcode attempts. This will result in the device resetting to factory defaults with all applications and data lost in the process. The device manufacturer may automatically impose time limitations after several unsuccessful passcode attempts before the wipe is triggered. ITS Support can provide assistance in resetting device passcodes.

7. Recommendations for Creating Compliant Passwords

In order to create a password that is compliant with the standards specified in this policy, consider creating a passphrase. A passphrase is similar to a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with a variety of character types is exponentially harder to breach than a shorter password. However, it is important to note that passphrases that are based on commonly referenced quotes, lyrics, or other sayings are easily guessable. While passphrases should not be famous quotes or phrases, they should also not be unique to the individual as this may make them more susceptible to compromise or password-guessing attacks.

- Choose a sentence, phrase, or a series of random, disjointed, and unrelated words
- Use a phrase that is easy to remember
- Examples:
  - Password: `When I was 5, I learned to ride a bike.`
  - Password: `fetch unsubtly unspoken haunt unopposed`
  - Password: `stack process overbid press`
  - Password: `agile stash perpetual creatable`

8. Password Reset Options

Various options are available to assist individuals with changing a forgotten or expired password. The preferred and fastest method is through the use of myAccount, the password management system. Individuals must be enrolled in Duo and have a personal email address on file in order to use this system to reset their password. A department administrator or the ITS Service Desk may assist with updating a personal email address, but individuals must provide proof of identity before any changes will be made.

8.01 Password Self-Service

Individuals can change or reset their password in the myAccount system. Individuals that know their current password and need to change it should click *Change Password*, authenticate with their current password, and acknowledge a Duo push request. Individuals who have forgotten their password will be required to validate their personal email address and acknowledge a Duo push request.

In the event your password cannot be reset via the myAccount system, individuals must contact the ITS Service Desk using one of the methods below.

8.02 In Person

Individuals who are local to the New York City area can visit the ITS SMARTDesk during normal business hours and present a non-expired, valid photo identification card, such as a driver license, passport, state identification, Weill Cornell Medicine identification, etc.) and supply a personal email address. The ITS technician should then reset the password escalate the case if necessary.

8.03 Video Conference

Individuals who are unable to visit the SMARTDesk in person or use myAccount to perform a self-service reset may conduct a video conference session with the ITS Service Desk if their computer or mobile device is equipped with a camera.

Affected individuals must contact the ITS Service Desk and request to setup a video conference using Zoom with the technician. The individual must then present their valid non-expired, valid photo identification card alongside their face to verify their identity over the video conference session. The technician will assist the individual with updating their personal email address and initiating the password reset process.

9. Reporting a Suspected Compromise, Security Incident, or Breach

Individuals who believe their password has been compromised or have been asked to provide their password to another individual, including ITS, should promptly notify any of the following support teams:

- ITS Security
  - Phone: (646) 962-3010
  - Email: its-security@med.cornell.edu
- ITS Support
  - Phone: (212) 746-4878
  - Email: support@med.cornell.edu
- Privacy Office
  - Phone: (212) 746-1179
  - Email: privacy@med.cornell.edu
- Cornell University Hotline
  - Phone: (866) 293-3077
  - Online: http://hotline.cornell.edu

Filing or reporting a security incident can be done without fear or concern for retaliation.

Revision History:

Date	Author	Revision
January 22, 2015	Brian J. Tschinkel	Updated policy template and language to conform with branding
August 23, 2016	Brian J. Tschinkel	Added video conferencing method for password resets
April 5, 2018	Brian J. Tschinkel	Updated mobile passcode parameters
November 18, 2020	Brian J. Tschinkel	Revised password policy parameters, added service and test accounts
April 18, 2021	Brian J. Tschinkel	Updated PCI account expiration parameters
September 5, 2023	Brian J. Tschinkel	Updated policy template, simplified language