


WCM Administrative Policy and Procedure		
 <b>Weill Cornell Medicine</b>	<b>Policy Title</b>	Password Policy
	<b>Policy Number</b>	ITS-500.15
	<b>Department/Office</b>	ITS Security
	<b>Effective Date</b>	January 22, 2015
	<b>Last Reviewed</b>	March 14, 2025
	<b>Approved By</b>	WCM-Executive Policy Review Group
	<b>Approval Date</b>	June 17, 2025

## Purpose

Assigning unique individual logins and requiring password protection is one of several primary safeguards employed to restrict access to the Weill Cornell Medicine (WCM) networks, systems, applications, and data. If a password is compromised, inappropriate access might be obtained by an unauthorized individual. Workforce Members are responsible for safeguarding against unauthorized access to WCM accounts, 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. This policy is 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).

## Scope

This policy applies to all WCM and WCM-Qatar Workforce Members who utilize WCM information technology resources and those responsible for managing and safeguarding WCM data.

## Policy

All Workforce Members are responsible for safeguarding Center Wide ID (“CWID”) and password credentials and must comply with the password standards identified in this policy. Passwords must not be used, stored, shared with, or made available to anyone in any manner that is not consistent with this policy.

## Definitions

**Hashing** - Is a way to change any piece of information into a shorter, unique representation of the original information.

**Peppering** – Technique used to protect passwords by adding a secret value to each password before it’s stored.

**Salting** – Technique used to protect passwords by adding a random string of characters to each password before it’s stored.

**Workforce Members** - Any faculty, staff, students, volunteers, trainees, and other persons whose conduct, in the performance of work for WCM, is under the direction and control of WCM, whether or not they are paid by WCM.

## Standards

### 1. Workforce Member Responsibilities

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

- Temporary or default passwords must be changed immediately upon first use.
- Initial passwords must be securely transmitted to the Workforce Member. By way of example, but not limited, encrypted email may be used.
- Unless otherwise provided for in this policy, passwords must never be shared with other Workforce Members or organizations. A compromised or suspected compromised CWID password is a reportable ITS security incident that must be reported to the Office of Compliance (OOC) by emailing [privacy@med.cornell.edu](mailto:privacy@med.cornell.edu) or ITS Security using one of the methods outlined in Section 8 of this policy.
- Nobody, including WCM Workforce Members, should ever 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 (unless otherwise provided for in this policy), the individual is obligated to report this to the OOC or ITS Security using one of the methods outlined in Section 8 of this policy.
- Passwords must never be written down or 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 as long as the master password is kept private and meets the requirements in this policy.
- Workforce Members must never leave themselves logged into an application or system where someone else can use their account.
  - To log into shared workstations (e.g., clinical exam rooms, kiosks), ITS will provide a limited-use shared account. Once logged into the shared workstation, an individual's own personal account must then be used for accessing applications, such as Epic. Shared accounts shall never be used to access applications.
  - 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 [WCM Policy ITS-500.01 – Responsible Use of Information Technology Resources](#), and their actions may be audited as needed.
  - In the event of a hardware malfunction and a 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. For managed systems, ITS can assist with this and other related processes. Passwords should never be shared with third-party repair providers.
- Workforce Members with access to limited-use, service, or test accounts must ensure the account password complies with this policy and keep the password stored in a secure manner.

- 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 in Section 8 of this policy.

## 2. Responsibilities of Systems Processing Passwords

All WCM systems—including, but not limited to, servers, applications, and websites that are hosted by or for WCM—must be able to accept, store, and transmit passwords with proper safeguards following this policy and industry best practices.

- Passwords should be prohibited from being displayed when entered, although it is suitable to have a method to manually toggle visibility as needed.
- Passwords must never be stored in clear, readable, or easily reversible formats like plaintext or Base64 encoding. 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 where supported. Hashing methods and configurations should follow industry best practices, such as using Argon2id or crypt.
- Hashed or encrypted passwords must never be accessible to unauthorized Workforce Members.
- 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. Appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized Workforce Members 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, if applicable, or immediately upon suspicion or confirmation of compromise;
- Not based on anything somebody could easily guess or obtain using person-related information (e.g., names, CWID, telephone numbers, dates of birth, hometown, other publicly available information, etc.);
- Not reasonably vulnerable to a dictionary or brute-force attack (see *Recommendations for Creating Compliant Passwords* below);
- Not reused for at least three (3) years; and
- Significantly dissimilar to any previous passwords.

### 3.1 Recommendations for Creating Compliant Passwords

To create a password that is compliant with the standards specified in this policy, consider creating a passphrase. A passphrase is like 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, such as city of birth, 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
- Put numbers or symbols in the middle instead of the end
- Examples:
  - Password: When I was 5, I learned to ride a bike.
  - Password: Fetch unsubtly 7 unspoken haunt
  - Password: stack 33 process Overbid
  - Password: !agile @stash #perpetual Creatable

## 4. Password Expiration

Most Workforce Members are not 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 reserves the right to immediately reset or expire an account's password, without providing prior notice, 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 WCM community who do not have privileged access to networks, systems, applications.

- All passwords must comply with the criteria herein.

### 4.02 Privileged Accounts

Privileged accounts have elevated access to administer networks, systems, and applications. These 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 immediately subsequent to each use.
- Privileged accounts that cannot be stored in the PAM system must have their passwords changed every ninety (90) days. Account owners are responsible for adhering to this requirement.
- All passwords must otherwise comply with the criteria herein.

## 5. Account Lockout

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

Workforce Members responsible for processing payments in WCM'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 accounts are used by a system, task, process, or integration for a specific and individual purpose. Test accounts are used on a temporary basis to imitate a role, person, or training sessions. 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, transmitting, or storing WCM data, such as smartphones and tablets, must 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. Password Reset Options

Various options are available to assist Workforce Members with changing a forgotten or expired password. The preferred and fastest method is through the use of [MyAccount](#), the password management system. Workforce Members must be enrolled in multifactor authentication (MFA) 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 Workforce Members must provide proof of identity before any changes are made.

### 7.01 Password Self-Service

Workforce Members can change or reset their password in the myAccount system. Workforce Members who have forgotten their password will be required to complete extra steps, such as validating their personal email address and acknowledging an MFA prompt.

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

### 7.02 In Person

Workforce Members who are local to the New York City area can visit the [SMARTDesk](#) during normal business hours and present a non-expired, valid photo identification card, such as a driver license, passport, state identification, WCM identification, etc.) and supply a personal email address. ITS may assist the individual with updating their personal email address, initiating the password reset process, or escalating the case if necessary.

### 7.03 Video Conference

Workforce Members 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. Workforce Members must enable their video and be prepared to display a non-expired, valid photo identification card. ITS may assist the individual with updating their personal email address, initiating the password reset process, or escalating the case if necessary.

## 8. Reporting a Suspected Compromise, Security Incident, or Breach

Workforce Members 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](mailto:its-security@med.cornell.edu)
- ITS Support
  - Phone: (212) 746-4878

- o Email: [support@med.cornell.edu](mailto:support@med.cornell.edu)
- o Online: [myhelpdesk.med.cornell.edu](http://myhelpdesk.med.cornell.edu)
- Office of Compliance: Privacy
  - o Phone: (646)-962-6930
  - o Email: [privacy@med.cornell.edu](mailto:privacy@med.cornell.edu)
- Cornell University Hotline
  - o Phone: (866) 293-3077
  - o Online: <http://hotline.cornell.edu>

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

## Compliance with this Policy

All WCM Workforce Members are responsible for adhering to this policy. Failure to comply will be evaluated on a case-by-case basis and could lead to corrective action, up to and including termination, consistent with other relevant WCM and University Policies. Instances of non-compliance that potentially involve a lapse of professionalism may lead to engagement of the Office of Professionalism for evaluation and intervention.

## Contact Information

Direct any questions about this policy, ITS-500.15 – Password Policy, to the Office of the Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-3609
- Email: [ciso@med.cornell.edu](mailto:ciso@med.cornell.edu)

## References

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- WCM Policy ITS-500.01 – Responsible Use of Information Technology Resources
- WCM Policy OOC-410.06 – Safeguarding Patient Information
- WCM Policy OOC-400.06 – Non-Intimidation and Non-Retaliation

## Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on 05/15/2025.
- WCM-Executive Policy Review Group (WCM-EPRG) on 06/17/2025.

## Version History

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

September 26, 2024	Office of the CISO	Updated policy template, simplified language
March 14, 2025	Office of the CISO	Updated policy template, revised language
June 17, 2025	Office of the CISO	Updated language and added new definitions. Assigned new policy number, "ITS-500.15." Formerly numbered, "11.15."