Password Policies and Guidelines

Policy Statement
All individuals are responsible for safeguarding their system access login ("CWID") and password credentials and must comply with the password parameters and 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 and procedure.

Reason for Policy
Assigning unique user logins and requiring password protection is one of several primary safeguards employed to restrict access to the Weill Cornell Medicine network and the data stored within it to only authorized users. If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously. 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 are designed to be complex and difficult to breach. The parameters in this policy are designed to comply with 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
Weill Cornell Medicine and affiliates with any type of WCM information system access.

Who Should Read this Policy
All individuals provided with a CWID for accessing Weill Cornell Medicine information systems.

Web Address of this Policy
https://its.weill.cornell.edu/policies/

Contacts
Direct any questions about this policy, 11.15 – Password Policies and Guidelines, 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) WCM passwords must be changed immediately upon issuance for the first-use. Initial passwords must be securely transmitted to the individual.

b) WCM passwords must never be shared with another individual for any reason or in any manner not consistent with this policy. A shared or compromised CWID password is a reportable ITS security incident.

c) Employees—including faculty, physicians, and supervisors—as well as students and other WCM personnel, must never ask anyone else for their password. If you are asked to provide your password to an individual or sign into a system and provide access to someone else under your login, you are obligated to report this to the Privacy Office or ITS Security using one of the methods outlined in the Procedures section below.

d) WCM passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices. 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 the 3. Password Requirements section of this policy.

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

   i. To access shared workstations (e.g., clinical exam rooms, kiosks), ITS will provide a limited-use shared account for the workstation. 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 his/her 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 his/her password with the technician. All ITS support technicians are expected to abide by the ITS 11.01 – Responsible Use of Information Technology Resources policy and their actions may be audited upon request.

   iii. In the event of a hardware malfunction and the device needs to be repaired by a third-party, the device hard drive should be backed up to a secure storage device and wiped securely prior to being handed over to an external technician. ITS can assist with a secure backup and the drive erasure and other exceptional circumstances. Passwords should not be shared with an external technician.

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

g) If a password needs to be shared for servicing, ITS Security should be contacted for authorization and appropriate instruction.

h) Passwords for WCM must be unique and different from passwords used for other personal services (e.g., banking).

i) WCM passwords must meet the requirements outlined in this policy.

j) WCM passwords must be changed at the regularly scheduled time interval (as defined in 4. Password Expiration where applicable) or upon suspicion or confirmation of a compromise.

k) Individuals with access to service accounts or test accounts must ensure the account password complies with this policy and must keep the password stored in a secure password manager.
I) In the event a breach or compromise is suspected, the incident must be reported to ITS Security immediately using one of the methods outlined in the Procedures section below.

2. Responsibilities of Systems Processing Passwords
All WCM systems—including servers, applications, and websites that are hosted by or for WCM—must be designed to accept passwords and transmit them with proper safeguards.

- Passwords must be prohibited from being displayed when entered.
- Passwords must never be stored in clear, readable format (encryption must always be used).
- Passwords must never be stored as part of a login script, program, or automated process.
- Systems storing or providing access to confidential data or remote access to the internal network must be secured with multifactor authentication.
- Password hashes (irreversible encoded values) must never be accessible to unauthorized individuals.
- Where possible, salted hashes (irreversible encoded values with added randomness) should be used for password encryption.
- 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 individuals have access to readable passwords.

3. Password Requirements
The following parameters indicate the minimum requirements for passwords for all individual accounts (except for passcodes defined in section 6. Mobile Devices) where passwords are:

- At least sixteen (16) characters;
- 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.); and,
- Not vulnerable to a dictionary attack (see section 7. Recommendations for Creating Compliant Passwords).

4. Password Expiration
Most users are no longer required to change their passwords at fixed intervals. Some account types, such as privileged users, must still adhere to regular password changes as defined below. However, in all cases, ITS Security reserves the right to reset a user’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 Users
Standard users consist of WCM faculty, staff (including temps and consultants), and students that are not (1) system administrators or (2) processing credit card payments.

- Passwords must be changed upon suspicion or confirmation of compromise.
- New passwords must comply with the criteria in section 3. Password Requirements.

4.02 Privileged Users
Privileged users consist of users with elevated access to administer information systems and applications (other than to a local device), most often in the Information Technologies & Services Department. Such users have administrator access via a shared account or to multiple systems at WCM and these accounts are at a higher risk for compromise.
Privileged domain accounts must be stored in the Privileged Access Management (PAM) system and passwords rotated upon each use.

Privileged accounts that cannot be stored in the PAM system must have their passwords changed every ninety (90) days.

Passwords must not be reused for at least six (6) generations.

Passwords must not be changed more than one (1) time per day.

At least four (4) characters must be changed when new passwords are created.

New passwords must comply with the criteria in section 3. Password Requirements.

4.03 Payment Card Industry (PCI) Users
Users 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 password expiration. As of this policy update, the requirements are below:

Passwords must not be reused for at least four (4) generations.

Passwords must not be changed more than one (1) time per day.

At least four (4) characters must be changed when new passwords are created.

New passwords must comply with the criteria in section 3. Password Requirements.

4.04 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 upon suspicion or confirmation of compromise.

Passwords must be changed when an account owner leaves the institution or transfers into a new role.

Passwords must comply with the criteria in section 3. Password Requirements.

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 user, as defined below.

5.01 Standard Users
Standard user 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 user’s identity is verified in order for the account to be unlocked sooner.

5.02 Privileged Users
Privileged user 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 user’s identity is verified in order for the account to be unlocked sooner.

5.03 Payment Card Industry (PCI) Users
Payment card industry (PCI) users have the following lockout policy:

• Accounts will lockout after six (6) 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 user’s identity is verified in order for the account to be unlocked sooner.

6. Mobile Devices
Mobile devices accessing or storing WCM data, such as smartphones and tablets, shall be registered with ITS and managed by the mobile device management (MDM) platform. The following minimum password policy is in effect for all mobile devices, where passwords are:

• At least six (6) digits;
• No repeating or sequential digits (e.g., 111111, 123456, or 101010); and,
• Changed every six (6) months.

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

A mobile device will erase after ten (10) invalid password attempts. The device manufacturer may automatically impose time limitations after several unsuccessful password 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 parameters specified in this policy, use one of the methods below.

7.01 Use 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 you 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
7.02 Use a Secret Code
A secret code can be used in conjunction with the previous methods simply by substituting letters for other numbers or symbols. Combining these methods will make it easy to incorporate the four character types in order to meet the password complexity requirements.

- Use a phrase that is easy to remember
- Capitalize the first letter of every word
- Substitute letters for numbers or symbols
- Incorporate spaces or substitute with a different character
- Example:
  - Phrase: “When I was five, I learned how to ride a bike.”
  - Password: WhenIwa$5,I1h0wt0rab1k3.

8. Password Reset Options
Various options are available to assist users with changing a forgotten or expired password. The preferred and fastest method is through the use of the password management system. You must be enrolled in Duo and have a personal email address on file in order to use this system to reset your password. A department administrator or ITS agent may assist you with updating your personal email address, but you must provide proof of identity.

8.01 Password Self-Service
You can change or reset your password in the myAccount system (https://identity.weill.cornell.edu). If you know your current password and need to change it, click Change Password to authenticate with your current password and acknowledge a Duo push request. If you have forgotten your password, you will be required to validate your identity by verifying your personal email address and acknowledging a Duo push request.

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

8.02 In Person
If you are local to the New York City area, visit the ITS SMARTDesk during normal business hours. Present a valid identification card (must contain a photo), such as a driver license, passport, state identification, WCM identification, etc.) to verify your identity and supply a personal email address. Reset your password with the ITS technician.

8.03 Video Conference
If you are unable to visit the SMARTDesk in person or use myAccount to perform a self-service reset, you may conduct a video conference session with ITS Support if your computer or mobile device is equipped with a camera.

Contact ITS Support during normal business hours and request to setup a video conference using Zoom with the agent. Present your valid photo identification card alongside your face to verify your identity. The agent will assist with updating your personal email address and initiate the password reset process.

9. Reporting a Suspected Compromise, Security Incident, or Breach
If you believe your password has been compromised or if you have been asked to provide your password to another individual, including ITS, promptly notify any of the following support teams:

- ITS Security
  - Phone: (646) 962-3010
  - Email: its-security@med.cornell.edu
11.15 – Password Policies and Guidelines

- **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.