Weill Cornell Medicine

11.15

Password Policies and Guidelines

Responsible Executive: Chief Information Officer, WCM
Original Issued:
Last Updated: April 5, 2018

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 meet the complexity requirements outlined and 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 the 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, Information Security Officer, using one of the methods below:

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

Contents

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:

- WCM passwords must be changed immediately upon issuance for the first-use. Initial passwords must be securely transmitted to the individual, either via the individual's supervisor or Human Resources at New Hire Orientation.
- 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.
- 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.
- 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 should not be stored in a web browser's password manager on an untagged device.
- Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.
    - To access multiuser 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.
    - 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.
    - 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.
- In the event that a password needs to be issued to a remote user or service provider, the password must never be sent without the use of proper safeguards (e.g., do not send passwords through email without encryption).
- If a password needs to be shared for servicing, ITS Security should be contacted for authorization and appropriate instruction.
- Passwords for WCM must be unique and different from passwords used for other personal services (e.g., banking).
- WCM passwords must meet the complexity requirements outlined in this policy.
- WCM passwords must be changed regularly, as outlined in this policy, at the regularly scheduled time interval or sooner if there is suspicion of a compromise.
- 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 should be secured with multifactor authentication.
- Encrypted password hashes must never be accessible to unauthorized individuals.
- Where possible, salted hashes should be used for password encryption. Exceptions should be filed and reviewed on a regular basis.
- Where any of the above items are not supported, 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 where passwords are:

- At least eight (8) 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.);
- Not vulnerable to a dictionary attack (see Recommendations for Creating Compliant Passwords section); and,
- Effective July 5, 2017, a combination of at least one character from each of the following four listed character types (older passwords require at least one character from three of the following four types):
    - English uppercase letters (A-Z),
    - English lowercase letters (a-z)
    - Base 10 digits (0-9)
    - Non-alphanumeric (such as ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . / and space)

4. Password Expiration

In order to prevent an attacker from making use of a password that may have been discovered, passwords are deemed temporary and must be changed regularly. ITS Security reserves the right to reset a user's password in the event a compromise is suspected or reported. The required frequency at which passwords must be changed varies based on the type of user, as defined below.

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 every six (6) months.
- 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 password requirements defined in the previous section.

4.02 Privileged Users

Privileged users consist of users with elevated access to administer information systems and applications, most often in the Information Technologies & Services Department. Such users have administrator access and these accounts are at a higher risk for compromise.

- Passwords must be 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 password requirements defined in the previous section.

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.

- Passwords must be changed every ninety (90) days.
- 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 password requirements defined in the previous section.

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 tagged 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) complex digits;
- No repeating or sequential digits (e.g., 111111, 123456, or 101010); and,
- Changed every six (6) months.

Fingerprint readers 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 three methods below.

7.01 Use a Passphrase

A passphrase is similar to a password, but it is generally longer and contains a sequences 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. Passphrases should be unique to you.

- Use at least twenty (20) characters
- Incorporate the four character types (a space or special character can be used to separate words or phrases in order to add complexity)
- Use a phrase that is easy to remember
- Abbreviate most of the words in the phrase to increase complexity
- Examples:
    - Phrase: "When I was five, I learned how to ride a bike."
    - Password: `When I was 5, I learned to ride a bike.`
    - Phrase: "When I was five, I learned how to ride a bike."
    - Password: `WheIwas5,Ilear2ridabik.`

7.02 Use an Acronym

An acronym can be used to constitute a strong and compliant password by taking the first letter of each word in a phrase (including punctuation) to form the password.

- Incorporate the four character types (forming your phrase in sentence case with punctuation can be used to meet the requirements)
- Use a phrase that is easy to remember
- Example:
    - Phrase: "When I was five, I learned how to ride a bike."
    - Password: `WIw5,Ilhwrab.`

7.03 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,Ilh0wt0rab1k3.`

A secret code can also be generated by using a keyboard pattern. Patterns can be generated by using geometric patterns, such as diagonal lines, series of lines, etc.

- Use a pattern that is easy to remember
- Incorporate letters, numbers, and/or symbols
- Enter passwords with caution as patterns may be easily visible
- Examples:
    - Pattern: a triangle starting with 'z' and incorporating an uppercase letter
    - Password: `Zse4rfvcx`
    - Pattern: the third, sixth, and ninth keys of each row, with one row of uppercase letters
    - Password: `369eyoDHLcn.`
    - Pattern: a series of lines, starting with %, r, d, and b, with one row of uppercase letters
    - Password: `%^&rtyDFGbnm`

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. Personalized security questions must be setup in order to use this system to reset your password.

8.01 Password Self Service

Login to myPassword (https://mypassword.med.cornell.edu) with your CWID and current password. (Users signing into the system for the first time will be prompted to setup an account.) If you have forgotten your password, you will be required to

validate your identity by answering security questions. Click “Change My Password” in the middle of the screen. Create a new password that complies with the parameters on the screen and in this policy. Use one of the methods described above to create a compliant password. Once your password has been changed, your password will synchronize across any service that is controlled by the ITS central authentication system (e.g., email, Windows logon, etc.).

In the event your password cannot be reset via the password management 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 at the WCMC Library Commons, 1300 York Ave, New York, NY 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. Reset your password with the ITS technician.

8.03 Video Conference

If you are unable to visit the SMARTDesk in person or use myPassword to perform a reset, you may conduct a video conference 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 WebEx or Skype with the agent. Present your valid photo identification card alongside your face to verify your identity. The agent will provide your temporary password to you over the phone and assist you with resetting it for future use.

8.04 Fax

As a last resort, you may send a password reset request to ITS Support via fax at +1 (646) 962-0669. Your request must contain (a) a copy of a valid photo identification card, (b) a signed note requesting your password reset, and (c) an alternate email address or phone number where you can be contacted. Once submitted, contact ITS Support to verify receipt of the fax and to reset your password.

9. Reporting a Suspected Compromise 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
- 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.

10. Definitions

These definitions apply to institutions and regulations as they are used in this policy. Definitions of technical terms are supplied by NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*.

- WCM — Weill Cornell Medicine
- ITS — Information Technologies & Services Department
- CWID — The Center Wide ID, (or “CWID”, pronounced “seaweed”), is a unique identifier consisting of a seven-character username assigned to all faculty, staff, and students. This ID is used to log into most major WCM and NewYork-Presbyterian computing systems. It also constitutes the first section of the WCM email address (CWID@med.cornell.edu or CWID@weill.cornell.edu). CWIDs usually consist of three initials of the user's name (first-middle-last, or for those with no middle name, two letters from the first name and one from the last) and a four-digit numeric identifier. (Faculty or staff who began employment with the institution prior to 1998 may have CWIDs that do not adhere to the current convention.) Only one CWID is assigned per person—it is deactivated when an individual leaves the institution, but it is never reassigned to someone else. The same CWID is used at both Weill Cornell Medicine and NewYork-Presbyterian Hospital and follows them if they change institutions.