Weill Cornell Medicine

11.17

Identity and Access Management

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: January 5, 2016
Last Updated: September 6, 2023
Last Reviewed: September 6, 2023

Contents

Policy Statement

Weill Cornell Medicine employs a number of administrative and technical controls in support of identity and access management. All members of the Weill Cornell Medicine community are expected to comply with these controls for providing, modifying, and terminating an individual's physical and logical access throughout their time at Weill Cornell Medicine.

Reason for Policy

This policy establishes standards and procedures to support the security and management of information assets and privacy of data in line with regulatory requirements.

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, 11.17 – Identity and Access Management, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

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

1. Identity Management

1.01 Person Types

Weill Cornell Medicine has identified several person types in support of identity management in order to assign identities among information systems. The following list of summarized person types are most common at Weill Cornell Medicine:

- non-academic employee
- academic employee
- academic non-employee
- affiliate
- student

1.02 Center Wide ID

The Center Wide ID, (or "CWID", pronounced "seaweed"), is a unique identifier consisting of a seven-character username assigned to any individual who, generally, is on the Weill Cornell Medicine campus, accesses a Weill Cornell Medicine system, or who needs to be tracked by a business unit.

For employment beyond 1998, a CWID issued by Weill Cornell Medicine generally consists of three letters from the individual's name (first initial + middle initial + last initial, or, for those without a middle name on file, first two letters from the first name + last initial) and a four-digit numeric identifier. Only one CWID is assigned per individual. The account associated with a CWID is deactivated when an individual leaves the institution, and CWIDs are never reassigned to someone else. The account associated with a CWID can be reactivated should an individual return to the institution after a period of inactivity or other absence. The same CWID is used at Weill Cornell Medicine, NewYork-Presbyterian Hospital (NYP), and Columbia University Irving Medical Center (CUIMC), even if employment or affiliation changes between the institutions.

The following list includes, but is not limited to, the types of individuals who will be assigned a CWID:

- employees
- academic staff
- voluntary faculty
- degree-seeking students
- non-degree seeking students
- visiting students
- alumni
- volunteers

An individual who already possesses a CWID from a prior affiliation with Weill Cornell Medicine, NYP, or CUIMC will not receive a new CWID. If an individual is affiliated with an institution where federated access has been established, a CWID is not required for applications equipped with federation.

1.03 CWID Creation

The process for assigning a CWID begins with the creation of an identity in one of the authoritative systems of record (SOR) overseen by various WCM departments:

- *Weill Business Gateway* (WBG) contains authoritative information about employees and is overseen by Human Resources

- *Academic Staff Management System* (ASMS) contains authoritative information about faculty and other academic appointments and is overseen by the Office of Faculty Affairs
- *Jenzabar* contains authoritative information about students and is overseen by the Office of the Registrar

Additionally, the *MARIA* system (Management of Access Rights and Identity Affiliations) allows for creation of identities for people who are of types not covered by the above SORs (e.g., vendors, contractors, volunteers, etc.) Such identity requests are made by department administrators via the *New Identity Request* form in MARIA.

These identities, along with the associated minimum information required defined below, are imported into the identity system. As warranted, Identity Management staff create new or assign existing CWIDs to these identities. An individual may have more than one active role at any given time, but those roles will all be associated with the same unique CWID assigned to that individual.

1.03.1 Minimum Information Required

The following data attributes are required to create a CWID:

- first name
- last name
- month and day of birth
- personal email address
- start date
- end date
- zip code
- mobile phone number
- requestor/sponsor CWID (for affiliates only)
- National Provider Identifier (NPI) (for health care providers only)

If an individual has an existing CWID issued by Weill Cornell Medicine, NYP, or CUIMC, this CWID should be supplied as part of the account creation process.

1.03.2 Activation

When an individual's faculty, staff, student, or affiliate role is activated in the identity system, the individual will receive a welcome email at their personal email address. This email contains instructions for activating their CWID.

To assist with onboarding, new academic employees and pre-matriculated students may be able to activate their CWID prior to their first working day, though access to Weill Cornell Medicine resources will be limited. Non-academic employees will not be able to activate their CWID prior to their first working day; any exceptions must seek approval from Human Resources.

1.04 Service Accounts

A **service account** is an account used by a system, task, process, or integration for a specific purpose. Requests for service accounts must include a desired name (following the standard naming convention with the svc- prefix), a Weill Cornell Medicine employee to serve as the sponsor/owner, a description of access rights requested, a valid business justification, and an expiration date (if applicable). Service accounts should not be used for interactive logon to systems as they provide little or no accountability for actions taken with this account. Passwords for service accounts must be securely generated, distributed, and stored in accordance with ITS policy 11.15 – Password Policy. Service accounts will be reviewed and recertified on a periodic basis in accordance with this policy.

2. Removal of Access Rights

The access rights of all individuals, including employees, students, academics, contractors, and third-parties, shall be (1) removed upon graduation or withdrawal, termination of their employment, , contracts or agreements, or (2) adjusted upon a change of employment, such as a transfer within Weill Cornell Medicine.

2.01 Scheduled Termination

Accounts shall be disabled within 24 hours of an individual's last working day. Student accounts shall be disabled with 90 days of their degree conferral date. Authorizations and entitlements shall be removed within 30 days of the account becoming disabled.

2.02 Immediate Termination

At the request and discretion of Human Resources, Office of General Counsel, Registrar, or ITS Security, an individual's access rights shall be immediately disabled following a notice of dismissal or in any situation where continued access is perceived to cause an increased risk to Weill Cornell Medicine. Authorizations and entitlements shall be removed within 30 days of the account becoming disabled.

2.03 Transfer

Changes of employment or other workforce arrangements, such as internal transfers within Weill Cornell Medicine, shall be reflected in removal of all access rights that are not appropriate for the new employment or workforce arrangement. At the request of the individual's previous or new management, inappropriate permissions shall be removed within 90 calendar days of the transfer, and new permissions shall be assigned.

2.04 Leaves of Absence

Individuals on a leave of absence may have their access rights reduced, suspended, or removed in accordance with the type of leave and expected work responsibilities.

- Academic staff on discretionary leave, such as sabbatical or personal leave, will be flagged as "On Sabbatical" in the Directory.
- Employees on various other types of leaves (e.g., military, disability, maternity/paternity, worker's compensation, etc.) will be hidden from the Directory.
- Students on leave (e.g., participating in a joint degree, academic remediation, special studies research, administrative hold, financial or health reasons, etc.) will also be hidden from the Directory.

In any situation, email access will remain active in order to foster communication. Access to clinical systems may be suspended and/or reinstated based on the type of leave. These accounts should remain in a reduced, suspended, or disabled state for the duration of the leave of absence and should be restored or re-enabled upon the individual's return to the institution.

2.05 Inactive Accounts

An inactive account is an account that has not been used for any purpose for a period of 180 days, including accounts for recently terminated individuals. A periodic audit, at least quarterly, should be performed by ITS to identify and remove redundant, unneeded, or inactive accounts. Inactive accounts should be disabled, and redundant or unneeded accounts should be deleted.

2.06 Other Account Credentials

If an individual knows passwords for active accounts or information assets, these passwords shall be changed upon termination or transfer.

3. Additional Offboarding Responsibilities

Upon termination or transfer of an individual at Weill Cornell Medicine, additional tasks (other than removal of access rights) must be completed in a timely manner and documented to signify completion. The individual's supervisor or the

respective department administrator is responsible for initiating a new offboarding workflow in the Offboarding Application (VPN required). Some of the important tasks include, but are not limited to, the following:

3.01 Building Access

All building identification cards which identify or associate the individual with Weill Cornell Medicine or its affiliates must be collected and securely discarded. Any office or facility keys which provide access to Weill Cornell Medicine- or affiliated-managed space must be collected and retained.

3.02 Electronic Equipment

Information systems associated with, assigned to, or primarily used by the individual must be inventoried and retained, unless prior written arrangements have been made, upon the individual's termination or transfer from Weill Cornell Medicine. The ITS asset management system can be used to assist with reconciling an inventory of the individual's electronic equipment. Common types of information systems include laptops, desktops, smartphones, tablets, servers, external or portable hard drives or flash media, CDs or DVDs, etc.

Individuals wishing to keep institution-owned computer equipment must have written approval from their department administrator and a completed ITS Asset Disposal Form. All systems must be appropriately sanitized and securely erased by ITS or disposed of through the Environmental Health & Safety electronic waste process in accordance with United States Department of Defense Standard DOD 5220.22-M.

Weill Cornell Medicine data stored on registered mobile devices (smartphones and tablets) will be remotely erased by ITS at time of termination.

Weill Cornell Medicine is not responsible for and does not guarantee that any personal data will be saved for, provided to, or made recoverable by an individual upon termination.

3.03 Custodial Access

Department administrators may request a supervisor or delegate to have access to a terminated individual's electronic files, including email, voicemail, and computer, after the individual's last working day at Weill Cornell Medicine. Custodial access requests can be submitted by department administrators in the Offboarding Application.

In some circumstances, custodial access may be granted for active individuals, including those on leave of absence, with approval from Human Resources or Office of General Counsel.

If the individual is transferring to another department or position within Weill Cornell Medicine, custodial access shall be limited to data relevant to the individual's exiting job responsibilities.

Revision History:

Date	Author	Revision
January 5, 2016	Brian J. Tschinkel	Initial version
November 23, 2021	Brian J. Tschinkel	Updated CWID creation, service account type, and recertified policy
September 6, 2023	Brian J. Tschinkel	Updated policy template, consolidated redundant sections