	WCM Administrative Policy and Procedure	
Weill Cornell Medicine	**Policy Title**	Identity and Access Management
	Policy Number	ITS-500.17
	Department/Office	ITS Security
	Effective Date	January 5, 2016
	Last Reviewed	June 2, 2025
	Approved By	WCM-Executive Policy Review Group
	Approval Date	September 23, 2025

Purpose

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

Scope

This policy applies to all Weill Cornell Medicine (WCM) Workforce Members and other individuals (collectively referred to as "individuals," unless otherwise specified) who utilize WCM information technology resources or individuals responsible for managing and safeguarding WCM data. Other individuals may include alumni, non-degree seeking students, WCM affiliates, etc.

Policy

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

Definitions

Center Wide ID (CWID): 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.

High Risk Data: Refer to WCM Policy ITS-500.03 – Data Classification.

Management of Access Rights and Identity Affiliations (MARIA): Is a system that allows for creation of identities for people who are of types not covered by the system of records (e.g., vendors, contractors, volunteers, etc.)

Systems of Records (SOR): A trusted information system that serves as the authoritative source for a specific set of data. It is responsible for maintaining the integrity, accuracy, and completeness of that data over time.

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.

Procedure

1. Identity Management

1.01 Person Types

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

- 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 WCM campus, accesses a WCM system, or who needs to be tracked by a business unit. The Identity and Access Management team is responsible for centralized oversight of WCM-issued CWIDs.

For employment beyond 1998, a CWID issued by WCM 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 by the end of the day 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 WCM, NewYork-Presbyterian (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 WCM, 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.

For employment entered before 1998, some of these CWIDs may differ from the standard three letter and four number convention.

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:

System	Authoritative For	Managed By
Weill Business Gateway (WBG)	Employees	Human Resources (HR)
Academic Staff Management System (ASMS)	Faculty and other academic appointments	Office of Faculty Affairs
Jenzabar	Students	Office of the Registrar
Non-Employee Application	Volunteers	Human Resources
Management of Access Rights and Identity Affiliations (MARIA) System	All other individuals	Department Administrators

Additionally, the MARIA system 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 WCM, 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 (or an email address for the user's current institution if that institution is an affiliate). This email contains instructions for activating their CWID. An additional email will be sent to instruct them how to enroll in Duo.

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 WCM 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 HR.

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 WCM employee serving as the sponsor/owner, a description of access rights requested, a valid business justification, and an expiration date (if applicable). Service accounts shall be assigned the minimum privileges necessary to perform their functions. Service accounts should not be used for interactive logon to systems. Passwords for service accounts must be securely generated, distributed, and stored in accordance with *ITS policy 500.15 – Password Policy*. The account's sponsor/owner Is responsible for reviewing the account's access privileges at least once per year, with more frequent reviews as necessary for High Risk Data and systems. Unneeded access rights shall be removed in a timely manner.

2. Review of Access Rights

Managers, supervisors, or department administrators are responsible for reviewing their team members' access privileges at least once per year, with more frequent reviews as necessary for High Risk Data and systems. Unneeded access rights shall be removed in a timely manner.

3. 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 WCM.

3.01 Scheduled Termination

All access rights, including authorizations and entitlements including physical badge access shall be revoked within 24 hours of the individual's last working day to mitigate security risks. All student access rights shall be disabled with 90 days of their degree conferral date. Authorizations and entitlements shall be permanently removed within 30 days of the account becoming disabled.

3.02 Immediate Termination

At the request and discretion of HR, Office of General Counsel (OGC), Registrar, or ITS Security, an individual's access rights and entitlements including physical badge access shall be immediately disabled following a notice of dismissal or in any situation where continued access is perceived to cause an increased risk to WCM. Authorizations and entitlements shall be removed within 30 days of the account becoming disabled.

3.03 Transfer

Changes of employment or other workforce arrangements, such as internal transfers within WCM, shall be reflected in the 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.

3.04 Leaves of Absence

Workforce Members 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.

1. Academic staff on discretionary leave, such as sabbatical or personal leave, will be flagged as "On Sabbatical" in the Directory.

2. Employees on various other types of leave (e.g., military, disability, maternity/paternity, worker's compensation, etc.) will be hidden from the Directory, but their existing access will not change.
3. 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, but their existing access will not change.

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.

3.05 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.

3.06 Other Account Credentials

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

4. Additional Offboarding Responsibilities

Upon termination or transfer of an individual at WCM, 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:

4.01 Building Access

All identification cards which identify or associate the individual with WCM, or its affiliates must be collected and shredded. Any office or facility keys which provide access to WCM - or affiliated-managed space must be collected and returned to the Campus Locksmith.

4.02 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 WCM. 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.

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

WCM 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.

4.03 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 WCM. Custodial access requests can be submitted by department administrators in the Offboarding Application. Department Administrators have the authority to designate a Divisional Administrator to perform this function using the Web Directory.

In some circumstances, custodial access may be granted for active individuals, including those on leave of absence, with approval from HR or the OGC.

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

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-500.17 – Identity and Access Management*, to the Office of the Chief Information Security Officer, using one of the methods below:

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

References

- WCM Policy ITS-500.03 – Data Classification
- WCM Policy ITS-500.15 – Password Policy
- WCM Policy HR 101 – Identification Cards United States Department of Defense Standard DOD 5220.22-M

Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on July 17, 2025.
- WCM-Executive Policy Review Group (WCM-EPRG) on September 23, 2025.

Version History

Date	Author	Revisions
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
September 26, 2024	Tom Horton	Updated policy template, clarified language
June 2, 2025	Office of the CISO	Updated policy template, defined ownership for identity systems, added Review of Access Rights section, clarified language. Assigned new policy number, “500.17” (formerly numbered 11.17).
September 23, 2025	Office of the CISO	Substantial updates to clarify instructions, responsibilities, and requirements.

Appendix

N/A