11.17

Identity and Access Management

Responsible Executive: Chief Information Officer, WCM
Original Issued: January 5, 2016
Last Updated: November 23, 2021

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 standards for providing, modifying, and terminating an individual’s physical and logical access throughout their tenure at Weill Cornell Medicine.

Reason for Policy
This policy establishes principles and provisions to support the security and management of information assets and privacy of data in line with regulatory requirements.

Entities Affected by this Policy
Weill Cornell Medicine

Who Should Read this Policy
All members of the Weill Cornell Medicine community who require or possess a CWID and/or have access to WCM facilities, information technology resources, systems, and 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
### Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 5, 2016</td>
<td>Brian J. Tschinkel</td>
<td>Initial version</td>
</tr>
<tr>
<td>February 8, 2022</td>
<td>Brian J. Tschinkel</td>
<td>Updated CWID creation, service account type, and recertified policy</td>
</tr>
</tbody>
</table>
1. Identity Management

1.01 Person Types
Weill Cornell Medicine (WCM) 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 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, accessing a WCM system, or who needs to be tracked by a business unit.

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 when an individual leaves the institution, but the policy is to never reassign a CWID to someone else. The account associated with a CWID can be reinstated should an individual return to the institution after a period of inactivity or other absence. The same CWID is used at both WCM, 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 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.

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 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)

If a user 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. This email contains instructions for activating their CWID.

To assist with onboarding, new hires may be able to activate their CWID prior to their first working day, though access to WCM resources will be limited. Some new 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 WCM 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 in accordance with ITS policy 11.15 - *Password Policy and Guidelines* and securely distributed to the account owner(s) using encryption. Credentials must be stored in a centralized password manager such as LastPass. 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 employees, students, academics, contractors, and third-party users of information and information assets shall be removed upon termination of their employment, graduation or withdrawal, contract or agreement, or adjusted upon a change of employment, such as a transfer within Weill Cornell Medicine.
2.01 Scheduled Termination
Upon termination, the access rights for the individual shall be disabled within 24 hours.

2.02 Immediate Termination
At the request and discretion of Human Resources, Office of General Counsel, or Registrar, an individual's access rights shall be immediately terminated following the supply of a resignation notice, notice of dismissal, or in any situation where continued access is perceived to cause an increased risk to WCM.

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 were not approved for the new employment or workforce arrangement. Access changes due to personnel transfer shall be managed effectively. Old permissions shall be removed within 90 days, and new permissions shall be assigned.

2.04 Leaves of Absence
Individuals on a leave of absence may have their access rights reduced 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.

2.05 Reduction of Access Rights
At the request and discretion of Human Resources, an individual’s access rights shall be reduced or removed prior to a termination or transfer. Such discretion shall be based on:

- whether the termination or change is initiated by the individual, or by management and the reason of termination
- the individual’s current responsibilities
- the classification and sensitivity of information assets accessible to the individual

2.06 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, shall be run by ITS to identify and remove redundant, unneeded, or inactive accounts. Any inactive accounts shall be disabled.

2.07 Suspended Accounts
A suspended account is an inactive account, except where the individual is on an extended leave of absence and is still actively affiliated with Weill Cornell Medicine. Such cases may include maternity/paternity leave, short- or long-term disability, sabbatical, etc. These accounts may remain in a disabled state for the duration of the leave of absence and may be re-enabled (restored) upon return to the institution.
2.08 Other Account Credentials
If an individual has known passwords for accounts or information assets remaining active, these shall be changed upon termination or transfer.

3. 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:

3.01 Building Access
All building identification cards which identify or associate the individual with WCM or its affiliates must be collected and securely discarded. Any office or facility keys which provide access to WCM- 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 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.

3.03 Custodial Access
Department administrators may request a supervisor or delegate to have access to a terminated user’s electronic files, including email, voicemail, and computer, after the user’s last working day at WCM. Custodial access requests can be submitted by department administrators in the Offboarding Application.

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

4. Additional Resources
- ITS Asset Disposal Form
- Offboarding Application (VPN required)

5. Related Policies
- 11.01 – Responsible Use of Information Technology Resources
- 12.1 – Integrity Policy
• 12.2 – Physical Security
• 12.3 – Authentication and Authorization
• 12.4 – Administrative Security