Weill Cornell Medicine

11.17

Identity and Access Management

Responsible Executive: Chief Information Officer, WCM
Original Issued: January 5, 2016
Last Updated: April 26, 2017

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 his/her 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, Information Security Officer, using one of the methods below:

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

Contents

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 WCM:

A. non-academic employee
B. academic employee
C. academic non-employee
D. affiliate
E. 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 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 Weill Cornell Medicine and NewYork-Presbyterian Hospital, 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 or is managed by NewYork-Presbyterian Hospital 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 creating a CWID for new academic and non-academic employees is instigated by Human Resources once applicable paperwork is completed. CWIDs for students are created through their respective programs. CWIDs for non-employees such as a temporary, voluntary, vendor, consultant, etc. are requested by the Department Administrators. Requests for a non-employee CWID (except students) may be submitted using the *Management of Access Rights and Identity Affiliations* (MARIA) system CWIDs for students are created based on data in the student information system.

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 Weill Cornell Medicine or NewYork-Presbyterian Hospital, this CWID should be supplied as part of the account creation process.

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 due to Severe Misconduct

At the request and discretion of Human Resources, an individual's access rights shall be immediately terminated following the supply of a resignation notice, notice of dismissal, etc. wherever continued access is perceived to cause an increased risk.

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 completing the Offboarding Checklist, including, but not limited to, the following tasks.

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 Asset Disposal Form. All systems must be appropriately sanitized and securely erased by ITS or through the EHS disposal process in accordance with United States Department of Defense Standard DOD 5220.22-M.

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

3.03 Custodial Access

Supervisors may request access to a terminated user's electronic files, including email, voicemail, and computer, after the user's last working day at WCM. Requests by a Department Administrator, Chair, or Director may be submitted to Human Resources for review. Upon approval, access will be granted to the designated custodian.

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

- Asset Disposal Form
- Offboarding Checklist

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

6. 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
- EHS Environmental Health & Safety Department