CORNELL UNIVERSITY
POLICY LIBRARY

Authentication to Information Technology Resources

POLICY 5.8

Volume: 5, Information Technology
Chapter: 8, Authentication to Information Technology Resources
Responsible Executive: Vice President for Information Technology and Chief Information Officer
Responsible Office: Office of Information Technologies
Originally Issued as Interim: January 20, 2006
Issued as Final: March 21, 2008
Last Updated: June 25, 2020

POLICY STATEMENT

Cornell University owns and manages university electronic identifiers. In the course of its business and missions, it provides its community with access to information technology (IT) resources, such as email, internet, and network devices through these identifiers. To protect these resources from unauthorized use, Cornell requires IT users to obtain electronic identifiers (specifically, Cornell electronic identifiers, as defined herein) to gain access to these resources, and follow specific rules for their use, as well as obtaining, changing, and terminating these identifiers. In addition, to avoid unauthorized access to IT resources, holders of Cornell electronic identifiers must follow specific rules for creating and using, and for reporting the suspected compromise of, complex passwords that correspond to a Cornell electronic identifier.

REASON FOR POLICY

Cornell University must protect its information technology (IT) resources and support regulations governing the privacy and security of sensitive data by requiring the use of electronic identifiers and secure passwords to control access.

ENTITIES AFFECTED BY THIS POLICY

- All units of the university. Weill Cornell Medicine and the Graduate School of Medical Sciences will administer and implement the policy under separate procedures.

WHO SHOULD READ THIS POLICY

- All members of the Cornell University community and others provided with Cornell electronic identifiers

WEB ADDRESS FOR THIS POLICY

- This policy: www.dfa.cornell.edu/policy/policies/authentication-information-technology-resources
- University Policy Office: www.policy.cornell.edu

Cornell Policy Library
Volume: 5, Information Technology
Responsible Executive: Vice President for Information Technology and Chief Information Officer
Responsible Office: Office of Information Technologies
Originally Issued as Interim: January 20, 2006
Issued as Final: March 21, 2008
Last Updated: June 25, 2020

POLICY 5.8

Authentication to Information Technology Resources

CONTENTS

RELATED RESOURCES

University Policies and Documents

University Policy 4.6, Standards of Ethical Conduct

University Policy 4.11, Establishing a New University-Related Subsidiary or Affiliated Corporation

University Policy 5.1, Responsible Use of Electronic Communications

University Policy 5.4.1, Security of Information Technology Resources

University Policy 5.4.2, Reporting Electronic Security Incidents

University Policy 5.7, Network Registry

University Policy 5.9, Access to Information Technology Data and Monitoring Network Transmissions

Campus Code of Conduct

Weill Cornell Medicine Policy 11.15, Password Policy and Guidelines

Weill Cornell Medicine Policy 11.17, Identity and Access Management

Weill Cornell Medicine Policy 12.3, Authentication and Authorization

Forms and Tools

Name	Description
How to Request a Sponsored NetID	Use to apply for a Sponsored NetID.
Guest ID Registration	Use to request a Guest ID.
Manage Your NetID	Use to activate a new Cornell NetID, change an existing password, or set your security questions for resetting a forgotten password.

CONTACTS

Direct any general questions about this policy to your college or unit's administrative office. Direct questions about specific issues to the following offices.

Contacts, Ithaca Campus Units

Subject	Contact	Telephone	Email/Web Address
Policy Interpretation and Clarification	IT Security Office	(607) 255-8421	security@cornell.edu it.cornell.edu/security-and-policy
Changing a NetID or a Forgotten Password	IT Service Desk	(607) 255-5500	itservicedesk@cornell.edu it.cornell.edu/support
Eligibility for a Cornell Electronic Identifier	Cornell Information Technologies Computer Access Administration	(607) 255-9853	computer_access@cornell.edu
Immediate Termination of a Guest ID	IT Security Office	(607) 255-8421	security@cornell.edu it.cornell.edu/security-and-policy
Immediate Termination of a NetID - Staff	Your Unit Human Resources Representative	Unit-specific	hr.cornell.edu/find-your-hr-representative
Immediate Termination of a NetID – Students	Office of the University Registrar	(607) 255-4232	univreg@cornell.edu registrar.cornell.edu
Immediate Termination of a Sponsored NetID	IT Security Office	(607) 255-8421	security@cornell.edu it.cornell.edu/security-and-policy
Security of Network Resources	IT Security Office	(607) 255-8421	security@cornell.edu it.cornell.edu/security-and-policy

DEFINITIONS: ITHACA CAMPUS UNITS

These definitions apply to terms as they are used in this policy.

Affiliate Staff	Employees of entities determined by University Policy 4.11, Establishing a New University-related Subsidiary or Affiliated Corporation, who qualify for a Cornell electronic identifier.
Applicant ID	Type of Cornell electronic identifier (see definition below) issued to prospective students who have submitted an application for admission.
Authentication	Process of verifying a user's identity when accessing information technology (IT) resources. Typically, identification is based on a user's Cornell electronic identifier and an associated password, personal identification number (PIN), or a card encoded with unique identification information.
Authorization	Process of granting a user access to IT resources and IT information based on predetermined access rights.
Central Authentication Infrastructure	System used to verify a user's identity when accessing IT resources.
Cornell Electronic Identifier	String of alphanumeric characters issued to users by Cornell Information Technologies (CIT) for the purpose of authentication to IT resources. Generally, there are four types of identifiers used at Cornell: Applicant IDs, NetIDs, Guest IDs, and Sponsored NetIDs.
Guest ID	Type of Cornell electronic identifier (see definition above) issued to guests of the university, who are not eligible for a NetID, but who may require access to restricted IT services. Guests may include conference attendees, visiting speakers, or vendor representatives, for example.
NetID	Type of Cornell electronic identifier (see definition above) issued to all new faculty, staff, and students, alumni, and affiliate staff.
Service Owner	Unit responsible for developing and maintaining IT products or services within a unit. Example: the Student Finance System, which is owned by the Bursar.
Sponsor	Unit head or designee requesting or providing a Sponsored NetID. (See definition below.)
Sponsored NetID	Type of Cornell electronic identifier (see definition above) issued upon the request of a unit head or a designee to individuals, such as independent contractors, who are not eligible for a NetID, but who provide services to the university.
IT User ("User")	Any individual who uses an IT device, such as a computer.

RESPONSIBILITIES: ITHACA CAMPUS UNITS

Admissions Office (Undergraduate or Graduate)	Request Applicant IDs for prospective students from the Cornell Information Technology (CIT) Identity Management Program Office.
Affiliate Business Office	Request NetIDs for new affiliate staff from the IT Service Desk.
Assistant Director of Cornell Information Technologies (CIT) Identity Management	Receive and review all requests to change a NetID, and make all final decisions on such changes.
Cornell Information Technologies (IT) Identity Management Program Office	Administer the online application through which Guest IDs are requested. Upon request by the Cornell Admissions Office, issue Applicant IDs to prospective students. Upon request by the university registrar, issue NetIDs to new students. Lead the design, development, and deployment of an authentication infrastructure. Work with the CIT Security Office to conduct risk assessments of the central authentication infrastructure.
Cornell Information Technologies (IT) Security Office	Conduct risk assessments of the central authentication infrastructure in cooperation with the CIT Identity Management Program Office. Terminate a Guest ID, and, in consultation with the sponsor, terminate a Sponsored NetID, when its use has been in violation of university policy.
IT Service Desk	Upon request by an affiliate business office, issue a NetID to an affiliate staff member. Upon request by a unit head or designee, issue a Sponsored NetID. Based on employment status information received from Human Resources (HR), terminate a staff, faculty, or affiliate staff member's NetID. Upon confirmation of student status with the university registrar, issue a NetID to a student walk-in. Upon request from the university registrar, terminate a student's NetID. Receive requests to change a NetID, and forward to the assistant director of Identity Management.
Office of Human Resource (HR) Records	Issue NetIDs for new faculty and staff. Provide employment status information to the IT Service Desk to immediately terminate a NetID for staff or faculty whose relationship with the university has ended or been suspended.
Office of the University Registrar	Request NetIDs for new students from the CIT Identity Management Program Office. Request termination of NetIDs from the IT Service Desk for students whose relationship with the university has ended or been suspended.
Unit Head/Sponsor or Designee	Request Sponsored NetIDs from the unit's security liaison. Annually renew Sponsored NetIDs.
Unit Security Liaison	Upon request from a unit head or designee, process requests for

RESPONSIBILITIES: ITHACA CAMPUS UNITS, CONTINUED

	Sponsored NetIDs, and submit them to the IT Service Desk.
Unit Supervisor or Human Resource (HR) Representative	Request NetIDs from HR Records for new faculty and staff. Request termination of NetIDs from HR Records for staff or faculty whose relationship with the university has ended or been suspended.
User of Information Technologies Resources (IT User)	Obtain and activate secure Cornell electronic identifiers and passwords to use when authenticating access to information technology resources. Apply established rules for password complexity when creating passwords accompanying Cornell electronic identifiers. Apply established rules for using passwords associated with Cornell electronic identifiers. Immediately change a password that may have been compromised. Report incidents in which a password has been compromised as outlined in University Policy 5.4.2, Reporting Electronic Security Incidents.

Cornell Policy Library
Volume: 5, Information Technology
Responsible Executive: Vice President for Information Technology and Chief Information Officer
Responsible Office: Office of Information Technologies
Originally Issued as Interim: January 20, 2006
Issued as Final: March 21, 2008
Last Updated: June 25, 2020

POLICY 5.8

Authentication to Information Technology Resources

PRINCIPLES

Overview

Cornell University owns and manages university electronic identifiers. In the course of its business and missions, it provides its community with access to information technology (IT) resources, such as email, internet, and network devices through these identifiers. To protect these resources from unauthorized use, Cornell requires IT users to obtain electronic identifiers (specifically, Cornell electronic identifiers, as defined herein) to gain access to these resources, and follow specific rules for their use, as well as obtaining, changing, and terminating these identifiers. In addition, to avoid unauthorized access to IT resources, holders of Cornell electronic identifiers must follow specific rules for creating and using, and for reporting the suspected compromise of complex passwords that correspond to a Cornell electronic identifier.

POLICY 5.8

Authentication to Information Technology Resources

PROCEDURES: ITHACA CAMPUS UNITS

Types of Cornell Electronic Identifiers

The university has established four types of electronic identifiers to be used when authenticating a user's identity to Cornell's IT resources.

- Applicant IDs
- NetIDs
- Guest IDs
- Sponsored NetIDs

◆**Note:** Possession of a Cornell electronic identifier does not, in and of itself, grant access to information or services. An individual's role or status with the university must determine the level of authorization granted. Data stewards and unit heads, or their service owners are responsible for establishing policies governing authorizing access to their services.

Creating Complex Passwords

To achieve security when authenticating to IT resources, the university has established the following rules for creating passwords associated with Cornell electronic identifiers, so that these passwords are complex enough to withstand attempts by unauthorized users to guess or decipher them.

Do	Don't
Choose at least eight characters, including at least three of the following four character types: • Uppercase letters • Lowercase letters • Numbers • Symbols found on your keyboard, such as ! * - () : | / ?...including blank spaces	Include your electronic identifier in your password Use words from the dictionary, including recognized names, such as "Cornell" Use names or nicknames of people, pets, places, or personal information that can be discovered easily, such as your name, spouse's name, address, birthday, etc. Include any of these: • Repeating characters, such as AAA or 555 • Alphabetic sequences, such as abc or CBA • Numeric sequences, such as 123 or 321 • Common keyboard sequences, such as QWERTY

POLICY 5.8

Authentication to Information Technology Resources

Protecting Passwords

To avoid unauthorized access to IT resources, users must apply the following rules for using passwords associated with a Cornell electronic identifier:

- Store the password in a secure location
- Use the password only to access services that use central authentication infrastructure enabled applications**.** For information about these applications, contact your unit security liaison
- Do not share the password
- Do not collect passwords from others or store them anywhere
- Do not share with anyone else the answers to questions used to reset forgotten passwords. To set a security question, use CIT's "Manage Your NetID" system (see Related Resources)

Obtaining a Cornell Electronic Identifier

Applicant IDs

University Undergraduate or Graduate Admissions will request Applicant IDs from the Cornell Information Technologies (CIT) Identity Management Program Office for prospective students who have submitted an application for admission to the university.

NetIDs

The college or unit human resource (HR) representative or the unit supervisor must request the NetID for new faculty and staff from HR Records. Affiliate business offices must request a NetID from the IT Service Desk for new affiliate staff. For new students, the university registrar must request the NetID from the CIT Identity Management Program Office. The new hire or student must activate his or her new NetID by visiting CIT's "Manage Your NetID" website. (See Related Resources.)

Faculty, staff, and students may each have only one NetID. Once a NetID is assigned to a user, it is never reassigned to another user. All NetIDs must be used only by the person to whom it is assigned. Students who become alumni may retain the use of their NetID from Cornell.

Guest IDs

Guests of the university who need access to restricted services may apply for a Guest ID using the online, self-service tool provided by CIT. (See Related Resources.) Upon submission of the request for a Guest ID, the user will receive e-mail instructions for activating it. If the Guest ID is not activated within a specific period, it will expire.

◆**Note:** Members of the university community must not use the Identity Management application to create Guest IDs for other users.

POLICY 5.8

Authentication to Information Technology Resources

PROCEDURES: ITHACA CAMPUS UNITS, CONTINUED

Sponsored NetIDs

Units that wish to sponsor an individual to obtain a Sponsored NetID must request the ID from the unit's security liaison. Possession of a Sponsored NetID must be essential to fulfilling the user's responsibilities to the university. The request must include the following:

1. Completed "Application for a Network Identity" form (see Related Resources.)
2. Photocopied, valid, government-issued photo ID card, such as a driver's license or passport
3. Printed letter of sponsorship on the sponsoring unit's official letterhead, signed by a university official (the sponsor). The letter must state the following:
    a. User's name
    b. Verification of the validity of the work being performed for Cornell and the business reason
    c. Necessity of a Sponsored NetID to do that work
    d. Certification that the sponsor will facilitate resolution of misconduct associated with the use of the NetID under his or her sponsorship

A sponsor may request only one Sponsored NetID per user. Once a Sponsored NetID is assigned to a user, it is never reassigned to another user. The sponsor must renew the ID annually, and must not be an immediate family member of the user being sponsored.

◆**Note:** Possession of a Sponsored NetID does not necessarily grant access to the same services available to staff members with NetIDs. Access to services is determined on a case-by-case basis according to specific criteria, such as vendor license agreements.

Changing a NetID

A NetID may be changed only under the following circumstances:

- The NetID was created incorrectly
- A health and safety issue exists related to the continued use of the NetID
- The user's legal name has been changed. (A legal document must be produced with the request)

Requests to change a NetID must be submitted in writing, stating the reason for the change, to the IT Service Desk, which will forward the request to the assistant

director for CIT Identity Management, who will review all requests, and make all final decisions on such changes.

Immediately Terminating a Cornell Electronic Identifier

Termination of a Cornell electronic identifier results in the immediate revocation of all access privileges belonging to the user of that identifier.

To initiate immediate termination of a NetID for a staff, faculty, or affiliate member whose employment with the university has ended or been suspended, the unit HR representative must contact the Office of Human Resources. The IT Service Desk will terminate a NetID upon request from the Office of Human Resources. In the case of students, the IT Service Desk will terminate a NetID upon request from the university registrar.

The CIT Security Office will terminate a Guest ID, or in consultation with the sponsor, a Sponsored NetID, if the use of the ID has been in violation of university policy.

Reporting a Compromised Password

A user who suspects that his or her password has been compromised must change it immediately using CIT's "Manage Your NetID" system (see Related Resources), and must report the incident as outlined in University Policy 5.4.2, Reporting Electronic Security Incidents.

INDEX