Policy 5.5
Emory Network IDs (NetIDs) and Passwords

Responsible Official: Enterprise CIO and Sr. Vice Provost for Library Services and Digital Scholarship
Administering Division/Department: LITS: Library & IT Services
Effective Date: March 14, 2007
Last Revision: August 22, 2013

Policy Sections:

Policy Details

Notice

All application systems should provide explicit notice to all users at the time of initial log in and regularly thereafter that:

- The system is a private system;
- It may be used only by authorized parties; and
- By successful log in, the user is acknowledging responsibility and accountability for his/her activities on the system.

Accountability

Each Network ID (netid) must have one individual who is responsible for all activity occurring as a result of the use of that netid.

Accounts

Default System Accounts

Whenever possible, the default account names for systems and applications (system and operator accounts) should be changed upon installation, implementation, and/or production use of systems and applications.

Inactive Network Accounts

- After ninety (90) consecutive days of inactivity, network accounts for faculty and staff will be disabled.
- For students, inactive network accounts will be disabled after six (6) months of inactivity.
- Users should be contacted prior to the disabling of a network account in order to ensure that accounts that have been inactive for justifiable reasons (illness, maternity leave, leave without pay, etc.) can be identified and held indefinitely in a suspended state.
- Otherwise, if, during the ten (10) days following notification of intent to disable, the user does not notify the Office of Information Technology of his or her request to keep the account (with a justified Emory use), or does not respond to the notice, the account will be disabled.

Inactive/Terminated Account Notification

- User network account databases should be routinely reviewed for network accounts of assigned users whose access purpose has ended.
- All such accounts should be deleted.
- Whenever an employee (or other individual assigned an Emory Network ID) leaves Emory or has a change in position

or other employment status, it is the responsibility of Human Resources and/or the department manager (or related position) to notify the the Office of Information Technology with a request to disable the account.

Network IDs (Netids)Authorization Accountability Standards for Network IDs (Netids)

- Identification of one individual responsible for each issued netid;
- Each netid must have one individual who is responsible for all activity occurring as a result of the use of the netid.
- Encouraging the use of the same netid across all Emory enterprise systems; and
- Creating a default framework for the assignment of netids.

Default Network IDs

- New netids on Emory Shared Data are created using default criteria. The current default netids for an individual, including a student eligible for a netids, consists of the initial of the individuals first name followed by up to six characters of the last name.
- To ensure there are no duplicate netids, the middle initial will be placed in the second position and/or numbers, as necessary, to the right of the name.
- Changes to an existing netids will not be made without a compelling reason (e.g., incorrect last name used in the netids, or netids is an offensive word). The new netids must include portions of both the user's first and last name.

Network ID Account Lockouts

- A netid account lockout occurs when a user can no longer log in to his/her computer or a specific application through the use of his/her netids. All account lockouts should be investigated.
- Accounts should not be unlocked until sufficient investigation has revealed the nature of the lockout.
- If an account has been locked multiple times during a relatively short time frame, the account should remain locked until a full investigation has revealed the source of the lockout attempts.
- In addition, every request for a network account password to be reset or for an account to be unlocked must be met by a challenge/response to verify the individual is authorized to the netids and/or account.

Sharing Network IDs

- The use of a netid by multiple individuals is strictly prohibited.

Passwords Aging Best Practice (Strongly Recommended)

- Passwords for Emory employees and contractors should expire every ninety (90) days, requiring the user to enter a new password before logging onto the system
- New passwords for Emory students should be required at the start of each semester
- System and operator user network accounts should be changed every thirty (30) days.

Passwords should also be changed if:

- User's machine has been compromised
- User has shared his/her password with any other individual
- User has been notified that his/her password does not meet current standards
- User has used the same passwords for 90 days or more

Display

- Keyed passwords must never echo or display in any readable form on the screen of the log in device.

History

- A history of previous user passwords should be maintained on all systems. This history file should be employed to prevent users from reusing passwords.
- The history file should remain encrypted at all times.
- Minimally, this history file should contain the last twenty-four (24) passwords for each user account
- Associated software should automatically reject any password selection that matches passwords currently held within the history file.

Length

- The length of passwords should always be checked for length automatically by the authenticating system at the time the user selects them.
- Passwords should be comprised of at least eight (8) to thirty-two (32) characters and should include both alphabetical and numeric characters, as well as at least one non-alphanumeric character.

Resets

Every request for resetting a user network account password or for unlocking an account should be met by a challenge/response to verify the individual is authorized to the account.

Remote Users

Remote users must authenticate through use of a valid Network ID and password in order to access the Emory network.

Related Links

- Current Version of This Policy: http://policies.emory.edu/5.5
- Change your Emory NetID Password (http://it.emory.edu/password/)

Contact Information

Subject	Contact	Phone	Email
Clarification of Policy	OIT Security Team	via listserv	securityteam-l@listserv.emory.edu

Revision History

- Version Published on: Aug 08, 2013 *(Changed password length and history depth into compliance.)*
- Version Published on: Aug 08, 2013 *(Added link to change your password)*
- Version Published on: Jan 18, 2011 *(Updated to remove old organizational names (such as AAIT).)*
- Version Published on: Mar 29, 2007 *(Original Publication)*