

UNC School of Medicine End User Account Policy

Overview

OIS provides central IT resources for the School of Medicine (SOM) such as electronic mail, shared file space and web services. People who are affiliated with the SOM may require an OIS-based account to access some of these resources. Since accounts are issued primarily to meet job-related needs, changes in responsibility may mandate changes to an account's privileges, and inactivity may indicate that the need for the account has expired.

Purpose

The purpose of this policy is to specify eligibility requirements for accounts, and the responsibilities of administrators, supervisors and users.

Scope

This policy covers accounts, authentication and authorization for all resources and servers managed by OIS.

Policy

A. General

An "account" (SOMid) consists of the user's ID and password required for the user to do business. The SOMid will be a three to eight character string, beginning with an alphabetic character, consisting of only lowercase letters or numbers, which is unique within the login domains supported by OIS. The password must be constructed in accordance with the SOM Password policy. A valid university PID will be associated with each account, to verify eligibility and to coordinate any communications with OIS Client Services.

B. Eligibility

The list of eligible affiliations is as follows:

- . Faculty and staff employed in Medical School departments
- . Adjunct Faculty
- . Students currently enrolled in the School of Medicine
- . Preceptors in the state who are actively hosting our medical students
- . Faculty-sponsored and collaboration-based users
- . Contractors and temporary personnel employed by Medical School departments

Exceptions will be reviewed on a case by case basis, and documented.

C. Account capabilities

An SOMid account provides a user access to a set of restricted resources, like email or web space. To provide diverse resources, OIS supports several "realms" of authentication, based on different hardware/software platforms. It may be necessary for a user to have several accounts to accomplish all job functions.

D. Consistent User Identifier (SOMid)

As much as possible, OIS will try to provide a consistent SOMid across its supported authentication realms. This includes trying to match SOMid's in Campus and Hospital domains. OIS will typically maintain two "public" mail aliases per account, a single "First_Last" alias and an alias for the user's SOMid.

E. Termination of Accounts

When a user leaves the SOM, his/her access to all accounts must be terminated as soon as practical but no later than 15 days after departure. Student email accounts will be terminated 90 days after graduation. The account SOMid will be reserved for six months before it can be issued to a different user. During this time, an email account may be put into "vacation reply" mode so that anyone sending mail to that address is informed of its status, a forwarding address if there is one, and possibly the user's "replacement" for work-related communications.

F. Change Notice

Accounts are issued because authorized access to resources is required. If the user's needs or employment status change, OIS must be notified by the supervisor. While it is in the users' best interest to report changes, it is the supervisor's responsibility to report relevant changes in employment status and authorization requirements to OIS. Account termination or reactivation requests will only be accepted from a supervisor. Where practical OIS will pursue notification from other sources to supplement information on accounts.

G. Account Inactivity

OIS maintains log files of access to most resources; because passwords must change every ninety days. If an account shows no activity for three months it may be disabled so that the user must contact OIS to reactivate it. An account that has been idle for six months may be removed without notice. A user who reactivates an account after it has been terminated will have the original SOMid reassigned if it is still available.

H. Account Abuse

Log files may also be scanned for indications of inappropriate use and/or resource abuse, for which an account can be terminated without notice.

Please note: there are active accounts which were created for groups that are no longer supported, which will be identified, notified and terminated. The list of historical affiliations no longer eligible includes:

Alumni (former medical students) who are not employed in the medical center
UNCLE accounts, created while OIS was hosting licensed resources
Hospital residents, who now require mail through the hospital AHEC librarians and other staff

Approved by the HIPAA Planning and Oversight Council (HPOC): April 27, 2004

Revision History

September 16, 2005