UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS

IT Account Management Policy

Policy #503

Source of Authority: N.C.G.S. 116-34(a);
UNC Code § 502(A)

Revision Authority: Chancellor

History: **First Issued:** February 17, 2011

Revised: May 1, 2017

Related Policies: Confidential Information Access (IT Security) Policy #501;
Email Policy #502;
Improper Activities Reporting Policy #114;
Takedown Notice Policy #507;
Technology Use Policy #508

Responsible Offices: Information Technology Department

Effective Date: May 1, 2017

I. Purpose

UNCSA relies heavily upon its computer information systems to meet operational, financial, educational and informational needs. It is essential that UNCSA's computer systems, and computer networks, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. It is critical that these systems and machines be protected from misuse and unauthorized access.

II. Scope

This policy applies to all faculty, staff, temporary employees, vendors, contractors, and affiliates of the University of North Carolina School of the Arts with access to computer and email systems.

III. Definitions

IV. Policy

A. **Exchange Email & Windows User Account Creation**

1. Normal account creation is done automatically by Human Resources process. Vendors, contractors, affiliates, and other special exceptions can be performed by the CIO/CTO and/or systems administrator.
2. Faculty/Staff are to have valid, authorized accounts and may only use those computer resources that are specifically authorized.
3. Access to special domain resources such as file servers or web servers is added by resource owners themselves or by system administrator with the permission of the resource owner/managers. Users are responsible for taking reasonable precautions to safeguard their own computer account.
4. Requests to create accounts must go to Human Resources. Special exceptions

require UNCSA sponsor and documentation for audit purposes.

B. Accounts can be suspended or disabled by the CIO/CTO or the systems administrator at the request of an authorized individual in response to a possible security vulnerability or reasonable suspicion of the violation of UNCSA Technology Use Policy.

C. The CIO/CTO may establish procedures and policies regarding account passwords and email storage space.

D. **Regulatory Limitations**

1. UNCSA may limit access when federal or State laws or UNCSA policies are violated or where school contractual obligations or operations may be impeded.
2. UNCSA may authorize confidential passwords or other secure entry identification; however, employees have no expectation of privacy in the material sent or received by them over UNCSA computing systems, networks, or stored on servers or workplace computing devices.
3. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above.

V. Revision History

A. February 17, 2011 – Adopted by Board of Trustees as part of UNCSA Policy Manual

B. March 26, 2012 – Revised to clarify that account users refers to faculty and staff.

C. September 13, 2016 – Revised to clarify the role of Human Resources in account creation.

D. May 1, 2017 – Revised to clarify retiree email account process and remove Director of IT.

UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS

IT Account Management Procedures

Procedure #503

I. Exchange Email & Windows User Account Creation

A. Accounts, access, and permission on the Windows domain/infrastructure are generated based on departmental templates by default.

B. Additional access or the inclusion in extra/special distribution lists is requested through email by department heads, department contacts, or distribution list owners.

C. Once an account is created, desktop support is notified to assist with initial machine setup and login.

D. The following individuals or their designees are authorized to originate requests for accounts to be created:

1. Human Resources
2. Dean's Offices (Hired Temporaries or Faculty)
3. CIO/CTO
4. Provost
5. Vice Chancellor for Business Affairs
6. Department Heads (for Temporaries within that department)

II. Email Account Suspension and/or Disabling.

A. In responding to possible security vulnerabilities or other reasonable suspicions of violation of UNCSA Technology Use Policy, an account may be disabled by email or phone request from the following or their designee:

- Executive Council
- Chief Information Officer/Chief Technology Officer
- General Counsel
- Deans
- Campus Police Chief
- Director of Information Technologies
- Network Administrator
- Systems Administrator
- One Card employee (termination notification)

B. Accounts are normally disabled by Human Resource process.

C. However, the systems administrator can disable an account involved in possible security vulnerabilities, or request of supervisor or department head.

D. Retirees and Emeritus Accounts

1. Faculty/Staff retirees in good standing are allowed to request their email address be forwarded to their personal email account – with no other system/file access – after retiring from UNCSA.
2. Emeritus Faculty are allowed to keep their UNCSA email accounts.
3. Each June 30, retiree accounts are examined for usage indicators.
4. If the account is not active during the fiscal year, the account is disabled.

III. Email/Windows Account Password

A. Passwords must be changed every 90 days.

B. Passwords have a 7-day minimum age.

C. There is a password history of 3.

D. The minimum password length is 8 characters.

E. Password resets for faculty/staff are typically managed by Help Desk, but can be performed by the systems administrator.

F. Requests for password resets can come directly from the faculty/staff member themselves, a departmental contact on their behalf, or from a member of IT on their behalf.

G. Positive identification and due diligence must be performed to ensure all password reset requests are legitimate and verified from a trusted source.

IV. Email storage space and file size restriction policy

A. Faculty/Staff email storage space and message size is limited.

B. Some incoming file types are filtered to prevent the spread of viruses and other malicious programs.