POL 08.00.02

Information Systems Management and Security Policy

**Authority:** Chancellor

**History:**

* First issued: November 5, 2001
* Revised: April 5, 2010
* Last revised: January 23, 2018

**Related Policies:**

* [NC General Statute §14-454 - Accessing computers](http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=14-454)
* [UNC Pembroke POL 07.45.01 – Misuse of State Property Policy](http://www.uncp.edu/about-uncp/administration/policies-and-regulations/all-policies/pol-074501-misuse-state-property-policy)

**Additional References:**

* [Office of the State Chief Information Officer – Statewide Information Security Manual](https://it.nc.gov/document/statewide-information-security-manual)
* [UNC General Administration Data and Records Retention Schedule](https://archives.ncdcr.gov/documents/university-north-carolina-general-records-retention-and-disposition-schedule)

**Contact Information:** Associate Vice Chancellor for Technology Resources and CIO,(910.775.4340)

**1. SCOPE**

1.1 This policy provides requirements for controlling access, both physical and electronic, to the technological and data assets of the university.

**2. ACCOUNTS**

2.1 Accounts are the means by which systems identify users and grant them access to resources. User accounts are created using established procedures and are locked, expired, disabled, or deleted in a timely manner when access is no longer authorized or required.

2.1.1 Only authorized users may access university technological and data assets.

2.1.2 Permanent employees and students are assigned network accounts upon hire or acceptance to the university. Accounts for specific systems requiring access beyond that of the network account will be granted in accordance with policy.

2.1.3 Temporary employees may be assigned accounts for the duration of their employment.

2.1.4 UNCP approved and recognized volunteers may be assigned accounts for the duration of their volunteer involvement.

2.1.5 Employees of other agencies or vendors are assigned accounts for the duration of their need for the account and only access necessary to the work being performed is granted.

2.1.6 Retired faculty and staff may apply for a retiree email account. Access to the retiree’s employee email account is disabled upon separation from the university.

2.1.7 Access to some applications require approval by the supervisor and appropriate data steward or manager.

2.1.8 Applications for group web accounts require approval from the university web master.

2.1.9 An individual user shall not use a generic account.

2.1.10 Supervisors may request access to the accounts of subordinates for the purpose of business continuity. Such requests require the approval of two levels of authority above that of the requestor. As such, deans, department heads and vice chancellors are normally included in the approval process.

2.2 Management of Accounts

2.2.1 All accounts assigned to an employee are expired or locked upon notification from Human Resources, or their designee, that the employee has separated from the university.

2.2.2 Adjunct faculty accounts are terminated upon notification from the appropriate dean. The academic deans will review accounts for adjunct and part-time faculty each spring and fall semester for continued activation and inform DoIT of changes in status.

2.2.3 An administrative account assigned to an employee may be expired or locked upon notification to DoIT from the appropriate data steward or manager that the employee no longer requires the account.

2.2.4 Access privileges on an administrative account are changed upon notification from the appropriate data steward or manager that the employee requires different access privileges.

2.2.5 Upon notification of an employee transfer by Human Resources, the appropriate data steward or manager shall be contacted to determine the continued need for an administrative account.

2.2.6 A group web account assigned to an employee is expired or locked upon notification that the employee no longer requires the account.

2.2.7 A student account is retained until the student graduates or has not enrolled for two consecutive semesters. Access to wireless, classroom, laboratory and residential networks shall be removed during the first normal semester in which the student does not enroll.

2.2.8 All users gaining access with unauthorized accounts, found compromising account security, or allowing unauthorized access may be subject to disciplinary action which may include dismissal.

2.3 Passwords shall be created and maintained per the DoIT Password Standard.

2.4 Enforcement

2.4.1 UNCP employees gaining access using another user’s account and password, found compromising account security, or allowing unauthorized access may be subject to disciplinary action which may include dismissal in accordance with federal, state and local laws and policies.

2.5 Privileged accounts on administrative systems

2.5.1 Privileged accounts on administrative systems have the potential to impact not only the operation of those systems, but also have a major impact on the entire university.

2.5.2 Where facilities permit, all activity in accounts with system privileges on administrative systems must be monitored.

2.5.3 Where facilities permit, all activity in accounts with production privileges and access to command procedures or source programs on administrative systems must be monitored.

2.5.4 Logs of monitoring activity must be maintained.

2.5.5 Where facilities do not permit monitoring as described in 2.5.2 and 2.5.3, above, alternative forms of controls must be employed.

**3. PHYSICAL SECURITY**

3.1 Physical security of data centers, network closets and end-user systems must be maintained at all times.

3.2Data Center access and security

3.2.1 Data center doors are to remain locked at all times.

3.2.2 Data center windows are to be screened to prevent access.

3.2.3 Normal office hours are Monday-Friday, from 8 a.m. to 5 p.m. At all other times, doors to offices adjacent to the data center(s) are to remain locked.

3.2.4 Only authorized personnel are permitted access to the data center(s).

3.2.5 DoIT personnel whose duties require routine access to the equipment within the data center(s) will be granted access to the data center. A list of these personnel shall be maintained by the data center manager.

3.2.6 Personnel and guests requiring occasional access to the data center(s) must be escorted by DoIT personnel. These personnel include housekeeping, maintenance or other university staff as well as vendor representatives.

3.3 Enforcement

3.3.1 Upon the approval of the Chief Information Officer or her/his designee, guests may tour the data center(s). Guests are to be supervised by DoIT employees with access to the combination at all times. No photography or videography allowed.

3.3.2 Any guest or personnel granted occasional access to the data center(s) must sign in and out whenever they enter and leave the data center.

3.3.3 UNCP employees found accessing these rooms without just cause, gaining access without following approved policy and procedure guidelines, compromising room security, or allowing unauthorized access may be subject to disciplinary action which may include dismissal in accordance with federal, state and local laws and policies.

3.4 Network closet access and security

3.4.1 Network closets allow direct access to network devices. They must be secured at all times.

3.4.2 Network closet doors are to remain closed and locked at all times.

3.4.3 Network closet windows are to be screened or barred to prevent access.

3.4.4 Only authorized personnel are permitted access to network closets.

3.4.5 DoIT personnel whose duties require access to the equipment within the network closets are granted access via the appropriate access method. A list of these personnel shall be maintained by the CIO or her/his designee.

3.4.6 In those cases where network closets are also used for other purposes, networking equipment must be secured within a locked cabinet.

3.4.7 Non-DoIT personnel desiring to gain entry into mechanical rooms that also serve as institutional data closets must check out the door key using normal key checkout procedures within Facilities Management.

3.4.7.1 While accessing the network closet, security of the doors must not be compromised in any manner nor should the door be left open without supervision. Unauthorized employees must not be allowed to enter the mechanical/network closet space. The individual checking out the key is accountable for the security of the mechanical/network closet space until the key is returned.

3.4.7.2 Non-university personnel must not be issued a key to any mechanical/network closet. Keys will only be issued to the responsible UNCP employee. The listing of UNCP personnel approved to obtain a key will be kept in the key log in Facilities Management. If the work is contracted, then the contractor is to be supervised by DoIT staff and/or Facilities Management staff during the work. The Facilities Management Director will review the key log file for compliance.

3.5 Enforcement

3.5.1 All access to the mechanical/network closet by UNCP personnel other than DoIT staff must be recorded as part of Facilities Management’s key check-out process. UNCP employees found accessing these rooms without just cause, gaining access without following approved policy and procedure guidelines, compromising room security, or allowing unauthorized access may be subject to disciplinary action which may include dismissal in accordance with federal, state and local laws and policies.

3.5.2 Upon the approval of the Chief Information Officer or the Deputy Chief Information Officer, guests may tour a network closet. Guests are to be supervised by DoIT employees. No photography or videography is allowed without express permission of the CIO or her/his designee.

3.6 Operator area access and security

3.6.1 The operator area is a place for operators to work containing valuable equipment and sensitive data. It provides access to the data center and must be secured at all times.

3.6.2 Normal office hours are Monday-Friday, from 8 a.m. to 5 p.m. At all other times, the doors to the operator’s area and adjacent offices are to remain locked.

3.6.3 All DoIT personnel are permitted access to the operator’s area during the normal office hours.

3.6.4 Other university staff, guests or vendor representatives whose duties require their presence in the operator’s area are to be supervised by DoIT staff at all times.

3.6.5 DoIT personnel should be aware of any visitors and monitor their actions.

3.6.6 DoIT personnel whose duties require access to the machine room are permitted to retain the combination to the operator’s area. A list of these personnel is maintained in the Office of the CIO.

3.7 Enforcement

3.7.1 UNCP employees found accessing the Operator Area or DoIT offices without just cause or gaining access without following policy guidelines, compromising room security, or allowing unauthorized access may be subject to disciplinary action which may include dismissal in accordance with federal, state and local laws and policies.

**4. RETENTION OF FILES FROM EXPIRED OR DELETED ACCOUNTS**

4.1 Although a user account may be expired or locked, data files stored in those accounts may be important to the university.

4.2 Files in individual directories from expired or locked accounts on administrative systems may be reviewed and copied by the appropriate data steward or manager or by application staff from DoIT.

4.3 The supervisor shall review and retain files on desktops or laptops from expired or locked accounts, as described in other policy. Hard drives are wiped before computers are disposed of or are imaged if the computer is to be reassigned to another user.

4.4 Files in individual directories on storage systems shall be reviewed and copied by the supervisor as described in other policy. The files shall be deleted in accordance with established record retention schedules.

4.5 Files in individual directories from expired or locked accounts on academic systems will be kept in accordance with data retention policies.

4.6 Files in individual directories from expired or locked accounts on Web systems will be kept in accordance with data retention policies.

**5. DATA RETENTION**

5.1 Various federal and state requirements exist that dictate the amount of time for which the [university must retain data.](https://www.northcarolina.edu/sites/default/files/records_retention_and_disposition_schedule.pdf) It is the responsibility of the employee’s former supervisor to ensure that data in an employee’s files are retained according to these requirements.

**6. ACCESS TO PROGRAMS AND COMMAND PROCEDURES**

6.1 Access to programs and command procedures has the potential to make a significant impact on the university. This impact includes risk associated with allowing access to confidential information, trade secrets or other materials under the constraints of a non-disclosure agreement. It also includes risk from users or intruders bypassing normal security methods to access or copy confidential information.

6.2 On administrative systems, read access to the source code of programs or command procedures shall be restricted to those administrators or developers whose duties require maintenance or support of the software.

6.3 On Web systems, read access to the source code of programs of command procedures shall be restricted to those administrators or developers whose duties require maintenance or support of the software.