ACCESS TO INFORMATION RESOURCES AND DATA
07.200.10

Authority:	Vice Chancellor Information Technology Systems
History:	Updated February 15, 2010; Reformatted June 6, 2005; supersedes policy ITS 2.00; effective September 11, 2002
Source of Authority:	Consolidated University of North Carolina Netstudy – Security Subcommittee Baseline Recommendations (Feb. 16, 2003); International Standard ISO27002
Related Links:	07.100 and 07.300
Responsible Office:	Information Technology Systems Division

I. Purpose

This document provides guidelines for responsible management of the access to information resources and data that support the primary administrative and academic functions of the university. The Information Technology Systems Division is responsible for managing access to ensure the integrity and confidentiality of these resources and data. This is not a comprehensive document covering all aspects of access management.

II. Policy

A. General Statement

Information resources and data that support the primary administrative and academic functions of the university are accessed through broad impact systems and software, and/or data sets stored and maintained on university servers. The management of broad impact systems and software for the university is the responsibility of the Information Technology Systems Division (see Management of Broad Impact Systems and Software). Management of the central campus computer systems is the responsibility of the Department of Operations and Systems Administration.   ITSD is responsible for ensuring the integrity and confidentiality of university information resources and data residing on broad impact systems and software on university servers.

1. Information Resources and Data

   a. For the purpose of this document, information resources and data refer to those resources and data that support the administrative and academic functions for the university and provide services to the campus community. They include databases, datasets, and files that contain information and data that are accessed through university broad impact systems and other software. This information is used by academic and administrative offices for official reporting, record keeping, and

performing the daily business of the university community.

III. Principles and Guidelines

A. Broad Impact Software Security and Integrity

1. IT Security in coordination with the appropriate data custodian is responsible for ensuring the data integrity and confidentiality such that access to the data is limited to the minimum required relative to job responsibilities of each individual or the individual's right to know. ITSD and the departments with specific data responsibilities for systems/applications and/or components of individual systems have instituted policies and procedures that address security and access controls ensuring confidentiality and integrity of information resources and data. These policies and procedures follow industry standard guidelines for information systems security and integrity, including COBIT standards. They address different levels of access and security as follows:

    i. The IT Security Office Systems Liaison for Security Administration is responsible for administering security for the SunGard Banner suite of administrative systems. This position performs periodic reviews and audits to ensure that the access granted to each individual continues to be limited to the minimum access required relative to job responsibilities of each individual or the individual's right to know.

    ii. UNCW Division Heads are responsible for verifying that the permissions granted to their subordinates are appropriate for the roles that they are assigned in order to perform the functions associated with their position annually in accordance with provisions set forth in NC State Auditor requirements. This is a control measure necessary to support UNCW Policy 01.230.

B. User accounts are controlled by the following guidelines:

1. Users are required to adhere to the UNCW 07.100 Responsible Use of Electronic Resources policy.

2. User's password information is for their exclusive use. Sharing password information will result in revocation of access privileges.

3. User access is limited to only those networked computer resources and privileges directly required to perform assigned duties, at the discretion of the appropriate Vice Chancellor, director or unit manager.

4. Accounts are generally limited to faculty (including adjunct and part time), staff and students of the University of North Carolina Wilmington. Accounts for contractors or time limited employees may be granted based on need established by the appropriate Vice Chancellor, director or unit manager.

5. Time limited user accounts will have an expiration date.

6. Service accounts may be allowed if they meet the following criteria

    i. Requested by department head or unit manager.

    ii. Serve a demonstrated need not achievable by other means.

    iii. A responsible person within the department or operating group is designated.

    iv. Highly restricted in regards to access to intradepartmental information only.

    v. No need exists to track any transactions the account may generate.

7. All user accounts are subject to password aging.

8. Blank passwords are not allowed.

9. User Accounts are locked out after five invalid login attempts.

10. Passwords are reset by computer operations staff.

11. Groups will be formed of users with a need for common resource access.

    Members of these groups will be added or removed at the request of the appropriate Vice Chancellor, director, unit manager or authorized designee.

12. Notice of Termination of employment received from Human Resources for faculty and staff will result in the user account being removed.

13. Student accounts will be removed when the student is no longer considered a student of the university.