07.100.01 USER ACCOUNTS AND AUTHORIZED ACCESS

Authority: Board of Trustees

History: Reformatted May 25, 2005; approved by Board of Trustees October 28, 2004; revised October 23, 2003; effective January 18, 2002

Source of Authority: Consolidated University of North Carolina Netstudy – Security Subcommittee Baseline Recommendations (Feb. 16, 2003); International Standard ISO17799


Responsible Office: Information Technology Systems Division

I. Purpose

A. The University of North Carolina at Wilmington strives to maintain access for its faculty, staff, and students (the "users") to local, national and international sources of information and to provide an atmosphere that encourages sharing of knowledge, creative processes and collaborative efforts within the University's educational, research and service missions. Access to these electronic information systems is a privilege, not a right, and must be treated as such by all users of these systems. All users must act honestly, responsibly, and prudently. Every user is responsible for the integrity of these information resources. All users must respect the rights of other computer users, and take care in acting responsibly to safeguard the security and confidentiality of electronic resources, information, and similar assets.

B. Users are responsible for all use of their computer account(s). They should make appropriate use of the system and network provided protection features and take precautions against others obtaining access to their computer resources. Individual password security is the responsibility of each user. Users should respect the policies of external networks and remote sites and only use facilities for which they have been authorized.

C. Users may not supply false or misleading data, nor improperly obtain another's password, in order to gain access to computers or network systems, data or information. The negligence or naiveté of another user in revealing an account name or password is not considered authorized use.

D. For the computers and network systems, all access privileges — including all accounts, user IDs, network IDs, telephone codes, and any other such access codes — are granted for exclusive and individual use of the individual to which they are assigned. Users may not allow or facilitate access to University computer accounts, equipment, restricted files or systems by
others. Users should not attempt to subvert the restrictions associated with their computer accounts.

E. When the user’s relationship with the University is terminated, he or she shall be denied further access to University computing resources. Authorized use also terminates unless extended by an appropriate university official.