USER ACCOUNTS AND AUTHORIZED ACCESS
07.100.01

Authority: CIO

History: Approved by the CIO August 1, 2019; Reformatted May 25, 2005; approved by Board of Trustees October 28, 2004; revised October 23, 2003; effective January 18, 2002

Source of Authority: UNC System Office Policy Manual, Chapter 1400 "Information Technology" International Organization for Standardization ISO/IEC 27002

Related Links: 07.300.01 Identity and Access Controls

Responsible Office: Information Technology Services

I. Purpose

Access to information technology systems is a privilege, not a right, and must be treated as such by all users of these systems. 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 information technology resources, information and similar assets.

II. Policy

A. Users are responsible for all use of their information technology account(s). They must make appropriate use of the system's and network's protection features provided and take precautions against others obtaining access to their information technology resources. Individual password security is the responsibility of each user. See UNCW Policy 07.300.01 Identity and Access Controls for additional information concerning password management. Users must respect the policies of external networks and remote sites and only use facilities for which they have been authorized.

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

C. All access privileges — including all accounts, user IDs, network IDs, PINs, and any other such identification or access information — are granted for exclusive and individual use of the individual to which they are assigned. Users may not allow or facilitate access to university information technology systems by others. Users must not attempt to subvert the restrictions associated with their accounts.

D. When the user's relationship with UNCW is terminated, he or she shall be denied further access to university information technology resources unless extended by an appropriate university official.