I. Purpose

A. Users are responsible for the security of their own account and password and are responsible for actions taken from their account. Users should keep their accounts secure and private. Users will use strong passwords when authenticating on to all University automated systems. Strong passwords are defined as eight or more characters with a combination of upper case, lower case, alphanumeric and special characters.

B. Users (faculty, staff and students) are responsible for the security and back-up of data stored on their individual desktops/laptops (including, but not limited to, e-mail and office files). Data is to be backed-up on media separate from the internal hard drive (such as USB drive, external hard drive or other removable media). The user is responsible for the safe and secure storage of all external back-up media. Data stored on centrally managed servers is automatically backed up.

II. Restrictions

A. Each user's individually owned programs and proprietary information are considered his/her property. Users shall therefore not attempt to access, read, copy, modify, distribute, replace, delete or otherwise make use of any other user's account or its contents, including data, directories, programs, files, disks or other information or software assets.

B. Users shall not access or attempt to gain access to any other system accounts or to any nonpublic or restricted portions of the UNCW network. Users also shall not intercept or attempt to intercept data or voice transmissions of any kind. Electronic resources shall not be used to attempt to circumvent or defeat any system or account security. Examples of activities of this type would include but not be limited to the use of any program or
procedure that is designed to: obtain other users' passwords; obtain access to restricted programs, systems or data; modify restricted programs, systems or data; obtain privileges beyond those initially granted to the user account. Forging, fraudulently altering or falsifying, or otherwise misusing university or non-university records (including computerized records, permits, identification cards, or other documents or property), or to possess such altered documents or files is also prohibited.

C. Users will not facilitate, support, cooperate with, or in any manner through action or lack of action assist others in the activities defined above. Neither shall electronic communications be used to steal another individual's works, or otherwise misrepresent one's own work.

D. The university has a right to expect that computer users will properly identify themselves. Computer accounts are assigned and identified to individuals. Users must not misrepresent themselves or send anonymous communications. All material prepared and utilized for purposes of university business and posted to or sent over university computing equipment, systems or networks must be accurate and must correctly identify the sender, unless a university administrator (department chair or higher) approves anonymity for a university business purpose. Users must provide proper and correct sender identification in all electronic correspondence within and leaving university electronic resources. Forging, fraudulently altering, or willfully falsifying electronic mail headers, electronic directory information, or other electronic information generated as, maintained as, or otherwise identified as university records in support of electronic communication is strictly forbidden. Adding, removing or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited.