shared resources.

5. Each User is expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.

6. Each User is expected to cooperate with the University to investigate potential unauthorized and/or illegal use of the University Network.

7. Each User is expected to respect the security and integrity of university computer systems and data.

III. P hibi i

A. Without limiting the general guidelines listed above, unless expressly agreed to by the Chief Information Officer, the following activities are specifically prohibited:

1. Users may not attempt to disguise their identity, the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or organization. Users may likewise not misuse or appropriate the University's name, network names, or network address spaces.

2. Users may not attempt to intercept, monitor, forge, alter or destroy another User's communications. Users may not infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of such other User.

3. Users may not use the University Network in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any computer, the University Network or any network that the University connects to, (b) interferes with the supervisory or accounting functions of any system owned or managed by the University, or (c) take action that is likely to have such effects. Such conduct includes, but is not limited to: hacking or spamming, placing of unlawful information on any computer system, transmitting data or programs likely to result in the loss of an individual's work or result in system downtime, sending "chain letters" or "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the work of others.

4. Users may not distribute or send unlawful communications of any kind, including but not limited to cyberstalking, threats of violence, obscenity, child pornography, or other illegal communications (as defined by law). This provision applies to any electronic communication distributed or sent within the University Network or to other networks while using the University Network.

5. Intentional access to or dissemination of pornography by University employees, temporary staff, contractors, or vendors is prohibited unless (1) such use is specific to work-related functions and has been approved the respective manager or (2) such use is specifically related to an academic discipline or grant/research project. This provision applies to any electronic communication distributed or sent within the University Network ord -10(t(t) -20(5u6 -20(5u6 -u6 -20(5u6 -u6 -21 (e) -20(5 (c) -20(31.5 (r) i6 -20(6 81472 (t) -20(5

materials, software, music or other media without the express permission of the copyright holder or as otherwise allowed by law. Information on the Digital Millennium Copyright Act can be found at: http://www.copyright.gov/legislation/dmca.pdf and the Copyright Act at: http://www.copyright.gov/title17/. Additional information may be found on the home page of the University's Copyright Committee (http://www.lib.unc.edu/copyright/).

2. disciplinary actions against personnel and students associated with the University,
