2.5 Inappropriate Activities.

The following apply to specific activities.

2.4.1 Illegal activity.

In general, it is inappropriate to store and/or give access to information on the University computing and networking facilities that could result in legal action against the University.

2.4.2 Objectionable material.

The University's computing and networking facilities must not be used for the transmission, obtaining possession, demonstration, advertisement, request or transmission of objectionable material knowing it to be objectionable material. This includes:

2.4.2.1 A film classified RC (refused classification), a computer game classified RC (refused classification), or a refused publication;

2.4.2.2 Child pornography;

2.4.2.3 An article that promotes crime or violence, or incites or instructs in matters of crime or violence; or

2.4.2.4 An article that describes or depicts, in a manner that is likely to cause offense to a reasonable adult.

- ❑ The use of violence or coercion to compel any person to participate in, or submit to, sexual conduct;
- ❑ Sexual conduct with or upon the body of a dead person;
- ❑ The use of urine or excrement in association with degrading or dehumanizing conduct or sexual conduct;
- ❑ Bestiality;
- ❑ Acts of torture or the infliction of extreme violence or extreme cruelty.

2.4.3 Restricted Software and Hardware.

Users should not knowingly possess, give to another person, install on any of the computing and networking facilities, or run, programs or other information which could result in the violation of any University policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password

2.4.3 Restricted Software and Hardware continued.

breakers, and packet observers. Authorization to possess and use Trojan horses, worms, viruses and password breakers for legitimate research or diagnostic purposes can be obtained from the Director of the Information Technology Center.

The unauthorized physical connection of monitoring devices to the computing and networking facilities which could result in the violation of University policy or applicable licenses or contracts is inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information. Authorization to possess and use such hardware for legitimate diagnostic purposes must be obtained from the Director of the Information Technology Center.

2.4.4 Copying and Copyrights.

2.4.4.1 Users of the computing and networking facilities must abide by the SUNO copyright policy, which covers copyright issues pertaining to University faculty, staff, and students as well as commissioned works of non-employees.

2.4.4.2 Respect for intellectual labor and creativity is essential to academic discourse. This tenet applies to works of all authors and publishers in all media. It includes respect for the right to acknowledgment and right to determine the form, manner, and terms of publication and distribution. If copyright exists, as in most situations, it includes the right to determine whether the work may be reproduced at all. Because electronic information is volatile and easily reproduced or altered, respect for the work and personal expression of others is especially critical in computing and networking environments. Viewing, listening to or using another person's information without authorization is inappropriate use of the facilities. Standards of practice apply even when this information is left unprotected.

2.4.4.3 In particular, users should be aware of and abide by the University policy on copying and using computer software. Most software that resides on the computing and networking facilities is owned by the University or third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the computing and networking facilities or for distribution outside the University; against the resale of data or programs, or the use of them for non-educational purposes or for

2.4.4.3 Continued

financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization. University employees who develop new packages that include components subject to use, copying, or redistribution restrictions have the responsibility to make any such restrictions known to the users of those packages.

2.4.4.4 With a greater emphasis on computer-based assignments, students need to be especially cognizant of the appropriate use of computing and networking facilities. In particular, academic dishonesty or plagiarism in a student assignment may be suspected if the assignment calling for independent work results in two or more solutions so similar that one can be converted to another by a mechanical transformation. Academic dishonesty in an assignment may also be suspected if a student who was to complete an assignment independently cannot explain both the intricacies of the solution and the techniques used to generate that solution. Suspected occurrences of academic dishonesty are referred to the Vice Chancellor for Student Affairs and the Vice Chancellor of Academic Affairs.

2.4.5 Harassment.

2.4.5.1 University policy prohibits sexual and discriminatory harassment. SUNO's computing and networking facilities are not to be used to libel, slander, or harass any other person. The following constitute examples of Computer Harassment:

- ❑ Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;

- ❑ Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

- ❑ Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided

2.4.5.1 Continued

reasonable notice that he or she desires such communication to cease (such as debt collection);

- ❑ Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another;

- ❑ Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

2.4.5.2 The display of offensive material in any publicly accessible area is likely to violate the University harassment policy. There are materials available on the Internet and elsewhere that some members of the University community will find offensive. One example is sexually explicit graphics. The University cannot restrict the availability of such material, but it considers its display in a publicly accessible area to be inappropriate. Public display includes, but is not limited to, publicly accessible computer screens and printers.

2.4.5.3 Southern University at New Orleans is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. Users are also cautioned that offensive, sexually explicit, and/or inappropriate material can inadvertently “pop-up” or otherwise appear on your screens or monitors without prior knowledge of its content. Having an e-mail address on the internet may lead to the receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk. Users using any e-mail services on University computers do so at their own risk.

2.4.6 Wasting Resources.

2.4.6.1 It is inappropriate use to deliberately perform any act, which will impair the operation of any part of the computing and networking facilities, or deny access by legitimate users to any part of them. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.