Last Updated:

Any access and use of computing, networking, telephoning, and information resources must not interfere with the University's instructional, research, health care and public service missions and should be consistent with the person's educational, scholarly, research, service, operational or management activities within the University.

Those who access and use University computing, networking, telephoning, and information resources are to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others, while acting to maintain a working environment conducive to carrying out the mission of the University efficiently and productively.

Responsibilities regarding system and resource use

Persons who access and use university computing, networking, telephoning, and information resources are responsible for:

- Respecting the rights of other individuals, including compliance with other university policies for students, faculty, and staff -- these rights include but are not limited to intellectual property, privacy, academic freedom, intimidation, insulting or harassing others, interfering unreasonably with an individual's work or educational performance, or the creation of an intimidating, hostile or offensive working/learning environment.
- Exercising caution when committing confidential information to electronic media.
- Uun(-1 (r)-4 (mpu)-8(il)6(v)-1 (n0 -21 (n i)2 ()-6(ne-6(h)1 ((r)-4 (k)2.9(3(v)-1 (n0 -2.-5 (s(l)-9 3 wi)

- You are responsible for the use of your account. You may not give anyone else access to your account. You must not use a Loyola network account that was not assigned to you. You may not try in any way to obtain a password or access code for another person's network account. You may not attempt to disguise the identity of the account or machine you are using. You must not attempt to circumvent access and use authentication, data protection schemes or exploit security loopholes without authorization.

Under no circumstances may individuals give others access to any system they do not administer or exploit or fail to promptly report any security loopholes. Individuals must act to maintain a working environment conducive to carrying out the mission of the University efficiently and productively. You are responsible for the security of your passwords and access codes. This includes changing them on a regular basis and keeping it confidential.

Individuals may not under any circumstances deliberately circumvent or attempt to circumvent data protection schemes or uninstall or disable any software installed by the university for the purpose of protecting the university from the intentional or unintentional disclosure of information.

Systems and network administration, and facilities management

Administrators of systems and networks are responsible for protecting users' rights, setting policies consistent with them, and publicizing them to their users. They have authority to control or to refuse access to anyone who violates these policies or threatens

but no more. University computing, networking, telephony and information resources are provided to support the University's missions in instruction, research, health care and public service. These resources may not be used for commercial purposes without authorization from the Vice President for Information Services. Please review the followi (p)-2 (o)-5d ( )1 (o)-5 (m-2 (s)-6( )19-8(/g)-4 (,)7ll. 2c(p)- (P)7.6(ol-42.aib18(/g)-4 (,) (n)-2)TJ-0.