Acceptable Use of Computing Resources Policy

The University is committed to providing secure yet open networks and systems that protect the integrity and confidentiality of information and data. The Office of Information Services is charged with providing the University community with the technological resources to deliver and support these commitments.

Each member of the University community is responsible for the security and protection of electronic information. Resources to be protected include networks, computers, software, and data.

All users are expected to act in a responsible, ethical, and lawful manner when using the University's information services resources. The following are examples, but are not an exhaustive list, of prohibited activities:

- Using the University's information services resources to attempt unauthorized use or interference with legitimate use by authorized users of other computers or networks, including misrepresentation of his or her identity to other networks (e.g. IP address "spoofing");
- Modifying or re-configuring of the software, data, or hardware of the University's information services resources (e.g. system/network administration, internal audit);
- Knowingly creating, installing, executing, or distributing any malicious code (including but not limited to viruses, worms, and spyware) or another surreptitiously destructive program on any of the University's information services resources, regardless of the result;
- Hacking into University computers or networks (this activity may be subject to prosecution by state or federal authorities);
- Unauthorized use or distribution of intellectual property or copyrighted material, including unauthorized peer-to-peer file sharing (this activity may be subject to prosecution by state or federal authorities, up to and including fines and/or imprisonment);
- Using a computer system attached to University resources to capture data packets (e.g. "sniffer");
- Launching denial of service attacks against other users, computer systems, or networks;
- Using the University's information services resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by state or federal laws is prohibited under this policy;
- Accessing (e.g. reading, writing, modifying, deleting, copying, moving) another user's files or electronic mail without the owner's permission regardless of whether the operating system allows this access to occur except in cases where authorized by the University;
- Knowingly interfering with the security mechanisms or integrity of the University's information technology resources (users shall not attempt to circumvent information technology protection schemes or exploit security loopholes);
- Connecting devices (e.g. switches, routers, hubs, computer systems, and wireless access points) to the network that are not approved by the Office of Information Services at the University (it should be noted that connecting through a University-provided authorization process is considered, by default, to be approved access);
- Connecting any device that consumes a disproportionate amount of network bandwidth;
- Intentionally physically damaging or disabling University computers, networks, or software without authorization;
- Intentionally sharing University passwords; and
- Using the University's resources for the production or viewing of pornography.

The University's informational resources are provided for use in conducting authorized University business. Using these resources for personal gain or for illegal or obscene activities is prohibited. Users observing any illegal activities must report their observance to an appropriate University official.

Abuse of networks or computers at other sites through the use of the University's resources will be treated as an abuse of the University's information technology resource privileges. Abuse of University policies, resources, or other sites through the use of information technology resources may result in termination of access, Honor Code violations, dismissal, legal action, and/or other appropriate disciplinary action. Notification will be made to the appropriate University office or local and federal law enforcement agencies. The Office of Information Services is authorized to isolate and/or disconnect computer systems from the network while assessing any suspected or reported security incident, in order to minimize risk to the rest of the University's network. This includes but is not limited to hospitals and clinics that may be involved in student education.