NYU POLYTECHNIC SCHOOL OF ENGINEERING

Information Technology/ Systems Policy Statement

Rationale

Information technology systems and electronic resources are provided with the understanding that the members of the School of Engineering community will use them with a sense of compliance / adherence to all applicable laws and regulations, mutual respect, cooperation and collaboration. These resources are finite, must be shared, and with an understanding that with any established interconnection of electronic resources, the effect of one individual can have a dramatic effect on others within the network. As such, the use of the University network and electronic resources is a revocable privilege. All constituents will benefit, if all users of the University's electronic systems, avoid any activities which cause problems for other users of the same systems. The School of Engineering reserves the right to monitor, limit, and restrict electronic messages, network/systems traffic, and the public or private information stored on computers owned, maintained, or managed by the School of Engineering. Computers not owned, maintained, or managed by the School of Engineering staff that abuse campus services may be denied access to campus resources. Email / voice mail, web pages, and digital content are subject to archiving, monitoring, or review, and/or disclosure by other than the intended recipient.

To that end, the School of Engineering expects that all individuals including, but not limited to, students, faculty, and staff, using its electronic resources will abide by the following policy statement

Acceptable Use Policy

All hardware, software, and related systems and services are provided by the School of Engineering for the sole purpose of enhancing and attaining the School of Engineering mission statement as outlined in the School of Engineering Strategic Plan, the student handbook, the institute's Code of Conduct, and other code of ethics / responsibilities documents. The School of Engineering expects all access to its systems to be authorized and pre-approved, and that users understand that laws currently exist that prohibit the following:

- Electronic libeling or defamation.
- Sending / Posting / Broadcasting messages that incite hate or discontent.
- Transmitting repeated unwanted advances.
- Falsifying information or impersonation.
- Unauthorized use, providing, or copying protected intellectual or copyrighted property.

The School of Engineering also states definitively that its network is a private network separate and distinct from the public Internet. As such, access and use must comply with all campus rules and regulations as well as compliance and adherence to all local, state, and federal laws. Examples of prohibited activities include but are not limited to:

- Posting or transmission of confidential or classified information.
- Use of offensive or discriminatory language.
- Transmission of graphic images, sounds or text that is sexual or offensive in nature.
- Sharing passwords with peers who do not own the account.
- Unauthorized use of other's passwords or accounts.
- Use of campus resources for personal profit or gain.
- Use of campus resources to harass, threaten, or otherwise invade the privacy of others.
- Initiate or forward email chain letters or messages.
- The installation or use of any servers on the network not expressly .approved by Information Services or the Administration.
- Deliberate attempts to cause breaches of network, servers, telecommunications systems or security or to examine network traffic
- Initiation of activities that unduly consume computing or network resources.
- Leaving your computer unlocked and unsupervised for extended periods of time

- Use of applications, for example P-2-P, to receive and/or distribute copyright materials, such as movies, music, and videos

The Information Systems Department proactively monitors the network for activity which violates the University Code of Conduct and Acceptable Use Policy. Failure to comply with the terms of this policy will be met with disciplinary or legal action in concert with the provisions as described in the Code of Conduct, code of ethics, and student / employee handbooks or other University policy documents. Penalties for unacceptable use range from immediate deactivation of the account through appropriate University judicial or disciplinary action or referral to law enforcement authorities.

Date:_____

Signature: _____

Print Name: _____