Acceptable Use of IT Resources (Network and Computing) Policy

Appendix B

Examples of the Acceptable Use of IT Resources

These examples are meant to assist the University community in the interpretation and administration of the Acceptable Use of IT Resources (Network and Computing) Policy. They are illustrative and not inclusive.

Network

Users are responsible for any traffic that appears on the network that originates from a network jack assigned to them, or from a wireless device that is theirs. For example, it is a violation:

- To use excessive network bandwidth (to check your quota, please see the webpage http://www.columbia.edu/cgi-bin/acis/networks/quota/netquota.pl)
- To attempt to deliberately degrade performance, deny service, or circumvent security mechanisms on any network.
- To violate the policies of external networks and resources.
- To distribute pornography to minors or to upload, download, distribute or possess child pornography.
- To violate export control laws and regulations of the United States.
- To use any University electronic information resources for unethical, illegal, or criminal purposes, or to damage any University resource, as well as other networks, resources, or accounts on other networks.
- To create or intentionally release computer viruses or worms, or to compromise a computer.
- To misrepresent, conceal, or attempt to conceal the origin or identity of any network device, traffic, or user.
- To use any University system or network as a vehicle to gain unauthorized access to other internal or external accounts, systems, or networks.
- To transmit a virus, worm, attack or other malicious software or process.
- To intercept or monitor any network communications not intended for you.

Computing

University computing resources include but are not limited to desktops, servers, kiosks, lab equipment etc. are all covered by the Acceptable Use Policy. For example, it is a violation:

- To share your account and password with someone else.
- To use or distribute copyrighted materials without authorization.
- To use or copy software without the proper licenses or make more copies of licensed software than the license allows (i.e. software piracy).
- To access licensed or restricted databases or other materials without authorization.

Acceptable Use of IT Resources Policy appendix B - revised 04-11.doc
• To use resources you have not been specifically authorized to use.
• To obtain, possess, use, or attempt to use someone else's password or access code regardless of how the information was obtained (e.g. voicemail boxes or password sharing.)
• To access accounts, files, data, messages, or processes without authorization, even if they are not securely protected (e.g. breaking into a system by taking advantage of security holes, or defacing someone else's web page.)
• To purposely look for or exploit security flaws for any purpose without permission from the CISO Office.
• To use computing or network resources for advertising or other commercial purposes.
• To use University resources to attack, deface, deny access to, harass, threaten, or otherwise do harm to other users or internal or external resources.
• To download or post to University electronic information resources, or transport across University networks, material that is illegal, proprietary, in violation of University contractual agreements, or otherwise is damaging to the institution.
• To use privileged access for anything other than official duties.
• To alter, corrupt, misuse, or destroy information without proper authorization.
• To use any means to hide your identity, or to interfere with other systems or users.
• To fail to report a possible security lapse and use a system under those conditions.

Privacy

Privacy violations have the potential to hurt other people. For example, it is a violation:

• To send private information (e.g., Social Security numbers, passwords, credit card, etc.) information of others via e-mail or to store it where it is visible to unauthorized individuals.
• To use electronic information resources for harassment or stalking other individuals.
• To eavesdrop on any technological means for communication (e.g. telephone, network traffic).
• To access or attempt to access another individual's electronic accounts, passwords, messages, data, applications, or systems.
• To access or copy another user's email, data, programs, or other files without the explicit permission of the owner.