Acceptable Computer & Network Use Policy

When using computing resources at the Laboratory for Fluorescence Dynamics (LFD), users are responsible for obeying the policies described in both this document and the policies of the University of California, Irvine, which can be found at http://www.policies.uci.edu/adm/procs/800/800-13.html and referenced documents.

UCI Computer and Network Use Policy
http://www.policies.uci.edu/adm/pols/714-18.html
- Network and Internet access at the UCI is a privilege and continued access requires that users act responsibly.
- Misuse of computing, networking, or information is unacceptable, and users will be held accountable for their conduct.

Examples of Misuse
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended solely for the purpose of damaging or placing excessive load on a computer system or network. This includes, but is not limited to, computer viruses, Trojan horses, worms, bots, flash programs or password cracking programs.
- Attempting to circumvent data protection schemes or uncover security loopholes without prior written consent of the system administrator. This includes creating and/or running programs that are designed to identify security loopholes and/or intentionally decrypt secure data.
- Using computers or electronic mail to act abusively toward others or to provoke a violent reaction, such as stalking, acts of bigotry, threats of violence, or other hostile or intimidating "fighting words." Such words include those terms widely recognized to victimize or stigmatize individuals on the basis of race, ethnicity, religion, sex, sexual orientation, disability, and other protected characteristics.
- Posting on electronic bulletin boards or web pages materials that violate University policy or codes of conduct.
- Attempting to monitor or tamper with another user’s electronic communications or reading, copying, changing, or deleting another user’s files or software without the explicit agreement of the owner.
- Violating terms of applicable software licensing agreements or copyright laws.
- Using campus networks to gain, or attempt to gain, unauthorized access to any computer system.
- Using a computer account or obtaining a password without appropriate authorization.
- Facilitating or allowing use of a computer account and/or password by an unauthorized person.
- Employing, either directly or by implication, a false identity when using an account or other electronic resources. This includes sending unauthorized mail that appears to come from someone else.
- Performing an act without authorization that will interfere with the normal operation of computers, terminals, peripherals, networks, or will interfere with others’ ability to make use of the resources.
- Using an account or service for any activity that is commercial in nature not related to work at UCI, such as consulting services, typing services, developing software for sale, advertising products, and/or other commercial enterprises for personal financial gain.
- Deliberately wasting computing resources, such as playing games while someone else is waiting to use the computer for UCI related work, sending chain letters, spamming, treating printers like copy machines, storing or moving large files that could compromise system integrity or preclude other users’ right of access to disk storage, etc.
Security Guidelines for Devices Connected to UClnet
http://www.policies.uci.edu/adm/procs/800/800-18.html

- Operating systems must be safely installed.
- Security patches must be installed and regularly maintained.
- Anti-virus software must be installed and kept up-to-date.
- Computers and network services must be protected by user IDs and good passwords.
- Unnecessary network services must be disabled.
- Firewall software supplied with operating systems should be configured and running.
- Anti-Spyware software should be installed and run periodically.

Additional Policies for using LFD Computing Facilities

- All computers and networked devices owned by the LFD are under control of the LFD system administrators, who may access user files or suspend services on the systems they manage without notice as required to protect the integrity of the network.
- The LFD and UCI perform occasional security audits. If a computer is found to be compromised or vulnerable to network attack, it will be disconnected from the network until its owner corrects the problem.
- MAC addresses and NetBIOS names of all networked devices must be registered with and approved by the LFD network administrators.
- Personal user accounts and/or passwords must not be shared. This includes LFD Active Directory accounts.
- No one who is not a UCI student or employee or official guest of the LFD may gain access to LFD computers, user files, user accounts, software, or internal network services.
- Users may not make publicly accessible any computing resources (computers, printers, files, software, etc.) other than through services offered by the LFD servers.
- Users may not install software, drivers, or services on public computers other than those needed for specific data acquisition tasks authorized by LFD staff.
- Software licensed by the LFD may not be copied or moved without permission by the LFD system administrators.
- Public computers, printers, network switches, and network cables may not be moved or unplugged without permission by the LFD system administrators.
- Wireless or wired network routers may not be installed.
- No incoming network services are allowed on any computer, except for those required for participation in Windows Networking, secure shell (sshd), and SSL encrypted remote desktop.
- Browse mastering, DNS, WinS, and DHCP services must be disabled on all computers.
- All computers will use DHCP for IP assignment. No other IP address may be used, nor may the IP address assigned by DHCP be used by anyone else on another computer. Statically assigned IP addresses may not be used without explicit permission.
- The only allowed network protocol is TCP/IP. IPX/SPX, NetBEUI, and AppleTalk network protocols must be disabled.
- The URL of the anonymous LFD FTP site may not to be published (e.g. in papers, reports, or web documents).

I have read and agree to adhere to the above policy

Signature: .............................................................. Date........................................

Print Name: .................................................................