

**LLE INSTRUCTION 9860E**

**SUBJECT: COMPUTER ACCESS POLICY**

**ENCLOSURE:** (1) Request for LLE Computer Access

1. **Purpose:** To promulgate computer access and security policy.
2. **Discussion:** LLE provides access to computational resources to support job-related activities of its personnel, students, and visitors. Access requires that users adhere to certain policies and procedures to ensure security and to prevent the corruption of system computational resources. Failure of users to adhere to these policies and procedures may result in the suspension of access privileges.

3. **Procedures:**

a. Privacy

All equipment used for computer operations at LLE, including computers themselves, mass storage devices, networking equipment, and media, is owned by LLE. While LLE is not responsible for the contents of files or database records stored by users, it reserves a right to access, by designated system administrators, any information contained in such files or records on any medium owned by LLE.

LLE also reserves the right to monitor any activity of the system for law enforcement or other purposes (including e-mail, web, chat, file transfers, or other communications over the network) to the extent required by law, to uphold contractual obligations, LLE policies, other applicable University policies, or to diagnose and correct technical problems.

b. Computer Security

- (1) All users are required to choose a secret password to access the LLE computer system. The password must be difficult to break, i.e., it should be 6 to 8 characters long, it should contain letters and digits, and some letters must be capitalized. Names or dictionary words should not be chosen for a password. The users must keep the passwords in strict confidence and not divulge them to anybody within or outside LLE. Under no circumstances will any member of the support staff ask a user to divulge a password by electronic mail or telephone.

- (2) To log onto one of the LLE Unix systems or to use LLE VPN, some users are given a SecurID card and must select a PIN code. Such users must handle the cards carefully, protect them from being stolen or lost, and never divulge their PIN to anybody. SecurID cards are the property of the University of Rochester and must be returned upon termination of the user account.
- (3) Users should not try to obtain access to any LLE account not explicitly granted to them by LLE system administrators or try to access, without permission from the owner, any information stored under any account other than their own.
- (4) Users should not take advantage of access to the LLE computer system to compromise any account or computing device inside or outside LLE.
- (5) Users should not install any files or software that circumvents proper user identification to access the LLE computer system.
- (6) Users should not intentionally download any files (images, movies, or software) that could be considered offensive or otherwise create a hostile working environment.
- (7) Users should not intentionally download any files and, by so doing, infringe upon the copyright, trademark, patent, or other intellectual property rights of others. The unauthorized storing, copying or use of audio files, images, graphics, movies, computer software, data sets, bibliographic records and other protected property is prohibited except as permitted by law.

c. Virus and Spyware Protection

The LLE Computer Support Group (CSG) installs anti-virus/anti-spyware protection software on all personal computers at LLE. The software must always be running when a computer is running. Users should not stop this software—even temporarily—and should alert CSG if they think the software is not running properly.

Users who remotely access LLE's network and computer systems through Virtual Private Networking (VPN) must use and keep up to date anti-virus/anti-spyware protection software. CSG will provide software for LLE owned computers that are used at home. While CSG can make suggestions, users are responsible for acquiring software for the personal computers they own.

VPN users must also ensure that all *Microsoft Update* **Critical** updates are applied on their remote systems as quickly as technically feasible.

d. Centralized Backup

Most of the LLE file systems including those on PC's are backed up, without users' intervention, every night. Users should not shut their personal computers off without prior approval of CSG. The LLE backup policies are published in the "Support" section of the LLE website under Computer/Documentation.

e. Use of Third Party Software

- (1) Users of PC's should not install or upgrade software on their machines. In particular, during Internet browsing, ActiveX controls should be disabled to prevent inadvertent downloads.
- (2) Copyrighted software can only be used on an LLE computer if proper licenses are acquired by LLE or if the license owner can, under the License Agreement, grant an LLE user access to such software. It is CSG's responsibility to de-install unlicensed software from any LLE computer whenever such software is discovered. Users should contact CSG if they have a reason to believe they have found copyrighted but unlicensed software on an LLE computer.

f. Data Confidentiality

It is the user's responsibility to ensure the confidentiality of any intellectual property or other confidential data used on LLE resources. The distribution, by any method, of any confidential or protected information used on LLE resources must first be approved by the Director's Office.

g. Access to Hardware

- (1) Users should not physically connect any computing or communications device, including wireless communications devices of any kind, to the LLE network without permission from CSG. Additionally, users should not open a computer box, change any settings, including hardware switches and BIOS parameters, install, upgrade, or remove any hardware component or driver. Users should never remove electric power from Unix workstations unless they have been instructed to do so by a member of CSG.
- (2) Users should not move non-portable computer equipment or install any equipment that may influence the physical environment of the computer site or obstruct access to the computing equipment without the approval of LLE computer Support.

h. Assistance

If users have any questions or need assistance with LLE computers, they should contact CSG. The pager number is published in the LLE phone list and also can be accessed through the web site on the Computer Support page.

i. Termination

When a user leaves the Laboratory for Laser Energetics, his or her computer access will be terminated unless the nature of the collaboration justifies an extension. In order to extend access, the user should contact LLE Administration. If approved, LLE Administration will notify CSG of the duration of the extension and what resources are to be made available.

4. **Approval**

Robert L. McCrory  
Director

**Laboratory for Laser Energetics  
Request for LLE Computer Access**

When a user leaves the Laboratory for Laser Energetics, his or her computer access will be terminated unless the nature of the collaboration justifies an extension. In order to extend access, the on-site investigator must complete the attached and the investigator and user must agree to abide by (3), (4), and (5) below.

1. The investigator must identify the nature of the collaboration (use attached).
2. The investigator/user must justify the necessity of using the University of Rochester, Laboratory for Laser Energetics computer resources in lieu of other resources at the location of the remote user (use attached).
3. Computer access will be granted only for work stated in (1) above.
4. The investigator/remote user may not at any time allow access to any other user. Additionally, the investigator/remote user must agree to comply with the University of Rochester and Laboratory for Laser Energetics policies attached.
5. The University of Rochester, Laboratory for Laser Energetics must be credited for work done on Laboratory for Laser Energetics computers.
6. If approved, the use of University of Rochester, Laboratory for Laser Energetics computer facilities will be limited to one (1) year unless the terms documented here are renewed.

I have read and agree with the Computer Access policy for the University of Rochester, Laboratory for Laser Energetics. I have attached the requirements stated in the policy and agree to abide by all rules and regulations. I understand that after one (1) year from the signing of this document, access to the University of Rochester, Laboratory for Laser Energetics computers will cease unless an extension is justified and approved prior to that date of termination.

\_\_\_\_\_  
Investigator

\_\_\_\_\_  
Remote User

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Print Department

\_\_\_\_\_  
Print Department

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

Approved:

\_\_\_\_\_  
LLE Deputy Director