LLE INSTRUCTION 9860F

SUBJECT: NETWORK ACCESS POLICY

ENCLOSURE: (1) Request for LLE Network Access

1. **Purpose:** To promulgate network 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 allows the use of certain approved personal portable devices. The use of such devices should comply with the rules outlined in this document.

      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 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 network. The password must be difficult to break, i.e., it should be a minimum of 8 characters long. It should contain letters, numbers, and symbols. 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. If a user calls Computer Support for assistance, Computer Support may, in rare cases, request the user password on the phone.

(2) To log onto one of the LLE Unix systems, to access Secure Global Desktop, or to use LLE Virtual Private Networking (VPN), some users are given a SecurID card and are required to 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 must never 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 must never take advantage of access to the LLE network to compromise any account or computing device inside or outside LLE.

(5) Users must never install any files or software that circumvent proper user identification to access the LLE network.

(6) Users must never intentionally download any files (images, movies, or software) that could be considered offensive or otherwise create a hostile working environment.

(7) Users must never 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. Remote Access

(1) Remote access to LLE Windows and UNIX desktops is provided through a Secure Global Desktop server (http://desktop.lle.rochester.edu). VPN access is only made available in cases where it is required for approved software to function properly.

(2) If a data collection device is installed at the user’s location (Google Screenwise for instance), email clients that connect to the LLE mail server must use SSL or TLS encryption.
d. **Virus/Spyware Protection and Software Updates**

The LLE Computer Support Group (CSG) installs anti-virus/anti-spyware protection software on personal computers owned by LLE. The software must always be running when a computer is running. Users should not stop this software—even temporarily—without approval from a member of CSG. Users are responsible for contacting CSG if they think the software behavior is unusual.

Users who are approved to remotely access LLE’s network and computer systems through Virtual Private Networking (VPN) or Secure Global Desktop (SGD) must use and keep up to date anti-virus/anti-spyware protection software. CSG will provide software for computers that are used at home.

Laptop users as well as home users of SGD and VPN must also ensure that all Microsoft Update Critical updates are applied on their remote systems as quickly as technically feasible. In addition, laptop and home users must also ensure that, at a minimum, the following programs are updated on at least a monthly basis: Acrobat (or Reader), Java, Firefox, Thunderbird, and Flash.

e. **Centralized Backup**

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

f. **Use of Third Party Software**

1. Users of LLE-owned desktop PCs should not install or upgrade software on their machines.

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 have a responsibility to contact CSG if they have a reason to believe they have found copyrighted but unlicensed software on an LLE computer.

g. **Data Confidentiality and Laptop Encryption**

It is the user’s responsibility to ensure the confidentiality of any intellectual property or other confidential data used on LLE resources or accessed remotely. The distribution to non-LLE destinations, by any method, of any confidential or protected information must first be approved by the Director’s Office. To limit
accidental exposure of confidential data, the following procedures must be followed:

(1) Any portable device that is configured to access LLE resources (such as email, network files or database records) must be password protected.

(2) Laptops, both PC and Mac, which leave the confines of LLE, must be encrypted with the University of Rochester approved disk encryption software.

(3) If possible, use Secure Global Desktop for remote access to confidential data as an alternative to storing information on portable devices.

(4) Exercise great care to physically protect portable devices and media.

h. Access to Hardware

(1) Users must never physically connect or disconnect 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, or 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.

i. Wireless Communications

(1) Users must disable wireless communications (except for Bluetooth) on any computer (such as a laptop) before it is connected to any of LLE’s physical networks.

(2) If users are hosting one or more visitors, they should direct them to connect to the UR_Guest WiFi Network. If a visitor needs a physical network connection, the user hosting them is responsible for making arrangements in advance with CSG.

j. Assistance

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

k. **Termination**

When a user leaves the Laboratory for Laser Energetics, his or her network access will be terminated unless the nature of the collaboration justifies an extension. In order to extend access, the on-site investigator should complete the enclosure LLEINST 9860F (Request for LLE Network Access). 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

30 November 2012
Laboratory for Laser Energetics
Request for LLE Network Access

When a user leaves the Laboratory for Laser Energetics, his or her network 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 Network 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 network 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