NERSC Computer Use Policies Form

The following is a list of general computer use policies and security rules that apply to all users of NERSC resources. Further information on NERSC security policies and practices can be found at http://www.nersc.gov/security/. Principal Investigators are responsible for implementing these policies and procedures in their organization and ensuring that users fulfill their responsibilities. *NERSC must have a signed copy of this form on file for every user.*

If you are reading this form online, please print out a copy; sign and return to NERSC (see fax and U.S. address below).

User Accountability

Users are accountable for their actions and may be held accountable to applicable administrative or legal sanctions.

Resource Use

Computers, software, and communications systems provided by NERSC are to be used only for DOE-sponsored work (as determined by the DOE NERSC Program Manager). Use of NERSC resources to store, manipulate, or remotely access any national security information is prohibited. This includes, but is not limited to, classified information, unclassified controlled nuclear information (UCNI), naval nuclear propulsion information (NNPI), the design or development of nuclear, biological, or chemical weapons or of any weapons of mass destruction. The use of NERSC resources for personal or non-work-related activity is prohibited. NERSC systems are provided to our users without any warranty. NERSC will not be held liable in the event of any system failure or loss of data.

Foreign National and Stateless Individual Access

A foreign national, as defined by DOE N142.1, is any person who is not a U.S. citizen, and includes permanent resident aliens. Access to NERSC resources is denied to any foreign nationals from countries on the Department of Commerce "Computer Tier IV" list. As of October 11, 2007, these countries are Cuba, Iran, North Korea, Sudan, and Syria. No work may be performed on NERSC resources on behalf of foreign nationals from Computer Tier IV countries. Stateless individual access to NERSC resources will be reviewed on a case-by-case basis. Principal Investigators are required to inform NERSC of any of their users who are foreign nationals or stateless individuals and their countries of citizenship. Access to NERSC resources by foreign nationals or stateless individuals that would involve a release of U.S. -origin software or technology will be reviewed by NERSC on a case-by-case basis.

Passwords and Usernames

A user identifier known as a username and password are required of all users. Passwords must be changed at least every six months. All passwords must conform to DOE Order 205.3 and NERSC guidelines which found at http://www.nersc.gov/nusers/accounts/password.php. Passwords must not be shared with any other person and must be changed as soon as possible after an unacceptable exposure, suspected compromise or by direction of a NERSC staff member.

Notification

Users must notify NERSC immediately when they become aware that any of the accounts used to access NERSC have been compromised. Users should promptly inform NERSC of any changes in their contact information.

Unauthorized Access

Users are prohibited from attempting to receive unintended messages or access information by unauthorized means, such as imitating another system, impersonating another user or other person, misuse of legal user credentials (usernames, passwords, etc.), or by causing some system component to function incorrectly.

Software Use

All software used on NERSC computers must be appropriately acquired and used according to the appropriate licensing. Possession, use or transmission of illegally obtained software is prohibited. Likewise, users shall not copy, store or transfer copyrighted software or data, except as permitted by the owner of the copyright.

Altering Authorized Access

Users are prohibited from changing or circumventing access controls to allow themselves or others to perform actions outside their authorized privileges.

Reconstruction of Information or Software

Users are not allowed to reconstruct or recreate information or software for which they are not authorized.

Data Modification or Destruction

Users are prohibited from taking unauthorized actions to intentionally modify or delete information or programs.

Malicious Software

Users must not intentionally introduce or use malicious software such as computer viruses, Trojan horses, or worms.

Denial of Service Actions

Users may not deliberately interfere with other users accessing NERSC or other system resources.

Data Retention

NERSC reserves the right to remove any data at any time and/or transfer data to other individuals working on the same or similar project once a user account is deleted or a person no longer has a business association with NERSC.

Account Usage

Users are not allowed to share their accounts with others.

Monitoring and Privacy

Users have no explicit or implicit expectation of privacy. NERSC retains the right to monitor the content of all activities on NERSC systems and networks and access any computer files without prior knowledge or consent of users, senders or recipients. NERSC may retain copies of any network traffic, computer files or messages indefinitely without prior knowledge or consent.

NERSC personnel and users are required to address, safeguard against and report misuse, abuse and criminal activities. Misuse of NERSC resources can lead to temporary or permanent disabling of accounts, loss of DOE allocations, and administrative or legal actions.

revision 1.1 date: 2007/October/11 20:06:56

Sign and return to NERSC:

```
by FAX (preferred):     (+1) 510-486-4248

by Postal Service:      NERSC Account Support, Lawrence Berkeley National Laboratory
                        One Cyclotron Rd., MS 943-256
                        Berkeley, CA 94720

 I have read the NERSC Policies and Procedures and understand my
 responsibilities in the use of NERSC resources.

Answers to all of the entries below are required, including NERSC Principal Investig

 Signature:

 Print Name:

 Citizenship:

 Organization:

 Email Address:

 Work Phone Number:

 NERSC Principal Investigator for one of your
        NERSC project accounts (repositories):

 Date:
```