

# Berkeley Lab Cluster Access Agreement

This form provides a subset of important policies, which govern your access to an LBNL resource. In addition, the RPM (in particular Section 9), State and Federal law, and applicable University policies apply. Additional information at: [lbl.gov/Workplace/RPM/](http://lbl.gov/Workplace/RPM/)

**IT must have a signed copy of this form for each user.  
Please sign the form in hardcopy and fax it to the number below. Do not email or otherwise electronically send the completed, signed form.**

The system you are being provided access to is for approved uses only as determined by the principal investigator and consistent with LBNL policies.

This system is only approved for unclassified, non-proprietary fundamental scientific research.

## **Computer Use**

Storage or processing of classified or sensitive information (including UCNI, NNPI, or any weapons-related work) is strictly prohibited and may be subject to civil and criminal penalties. You have no expectation of privacy in your use of this system. Your actions, history, and user-data are subject to inspection and review by authorized parties per LBNL Policy. LBNL may share this information with law enforcement at its discretion.

No incidental personal use is permitted on LBNL Clusters.

This system is provided without warranty or set service level. LBNL will not be held liable in the event of any system failure or loss of data.

## **Data Retention**

When a user account is deleted, all permanent files (in home directories and LBNL cluster systems) are assigned to the PI, who is responsible for deleting unneeded files.

## **User Accountability**

You are accountable for your actions. Sanctions for policy violations may include termination of access, and civil and criminal penalties.

A user identifier (username and password) is required of all users. You must adhere to LBNL password guidelines. Passwords must not be shared. The password must be changed as soon as possible after an unacceptable exposure or suspected compromise.

## **Access**

Passwords are checked for integrity on a regular basis. It is the user's responsibility to maintain a strong password that conforms to the LBNL password policy as per [RPM policy](#). Accounts with weak passwords or passphrase less keys will automatically be deactivated upon discovery for security reasons. LBNL is not obligated to notify users prior to account deactivation if they have violated the password policy.

Users may be required to use a one-time password-generating device to gain access to their clusters. Users are not allowed to offer the OTP credentials to any other third party or host other than the LBNL clusters they are authorized to access

## **Best Practices**

Users are not allowed to list their username, hostname and OTP credentials (PIN) on the OTP device.

Users are asked to access the clusters directly from their workstations and laptops and avoid using other hosts as intermediate hops.

Users should not leave their login sessions open and idle for long periods of time and should lock their screens while away from their workstations and laptops.

## **Unauthorized Access**

Users are not to attempt to receive unintended messages or access information by some 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 LBNL computers must be appropriately acquired and used according to the appropriate licensing. Possession or use of illegally copied 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 or to circumvent security systems.

**Data Modification or Destruction** Users are prohibited from taking unauthorized actions to intentionally modify, delete, or reconstruct information or programs.

**Malicious Software** Users must not intentionally introduce or use malicious software such as computer viruses, Trojan horses, or worms. Users are responsible for taking reasonable steps to ensure the integrity and security of software they introduce to the system.

**Denial of Service Actions** Users may not deliberately interfere with other users accessing system resources.

**Notification** Users must notify LBNL immediately when they become aware that any of the accounts used to access LBNL have been compromised. LBNL reserves the right to temporarily disable accounts without prior notification in the event of a security compromise.

**Account Usage** Each user of this system must have a unique login. Users are not allowed to share their accounts with others.

**IMPORTANT:** The number one threat to this cluster is from a compromised endpoint (like your desktop computer) which allows your username/password to be stolen or your session to be hijacked. You are responsible for taking reasonable steps to ensure the security of any system you use to access LBNL systems.

### **Sign and return to LBNL:**

by FAX to (+1) 510-486-4107

**OR** by Postal Service to: HPCS Account Support / Lawrence Berkeley National Laboratory, One Cyclotron Rd. , MS 50B-2232, Berkeley, CA 94720

**I have read the LBNL Policies and Procedures and understand my responsibilities in the use of cluster resources managed by the LBNL IT Division.**

|                                   |  |
|-----------------------------------|--|
| <b>Signature:</b>                 |  |
| <b>Print Name:</b>                |  |
| <b>Organization:</b>              |  |
| <b>Email Address:</b>             |  |
| <b>Work Phone Number:</b>         |  |
| <b>Principal Investigator:</b>    |  |
| <b>Date:</b>                      |  |
| <b>Crypto Card Serial Number:</b> |  |