Livermore Computing Policies and Procedures

Lawrence Livermore National Laboratory •PO Box 808, L-63 •Livermore CA 94551 •Fax (925) 422-0592

This is a list of general computer use policies and security rules that apply to all users of Livermore Computing (LC) computers or networks. Principal Investigators are responsible for implementing these policies and procedures in their organization and ensuring that users are aware of their responsibilities. Principal Investigators are required and users are advised to retain a copy of this document for reference and audit purposes.

Users are notified that all LLNL computers and networks are monitored by the LLNL Computer Security Organization to insure proper computer use and to protect against attacks. Any evidence of criminal activity will be turned over to the proper law enforcement agencies. All data and files processed on or stored on LC computing resources will be periodically copied to archival storage. Members of the LC administration staff may review these copies and all programs and data on LC computers at any time.

Computer Use

Computers, software, and communications systems provided by LC are to be used only for DOE-sponsored work. The use of this equipment or software for personal or non-DOE-work-related activities is prohibited.

User Accountability

Users are accountable for their actions and may be held liable to administrative, civil, or criminal sanctions for any unauthorized actions found to be intentional, malicious, or negligent.

Passwords and User IDs

A user identifier, known as a User ID and password, are required of all users. LC accounts will be associated to a One Time Password (OTP) token where available. Otherwise, it will meet the DOE-specified password requirements as specified in LLNL CSP Policy 2430. Passwords must be changed every six months if not linked to an OTP. Passwords must not be shared with any other person and they must be changed as soon as possible after an unacceptable exposure or suspected compromise.

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 (User IDs, passwords, etc.), attacking the system, installing a network monitor (sniffer), or by causing some system component to function incorrectly.

Software License

All software used on LLNL computers must be appropriately acquired and used according to the appropriate licensing. Possession or use of illegally copied software is prohibited.

Malicious Software

Users must not 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 system resources.

Data Modification or Destruction

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

Reconstruction of Information or Software

Users are not allowed to reconstruct or re-create information or software for which they are not authorized.

Home Directory Policy

A user's home directory is created with permissions set so that only the user can access files and subdirectories within their home directory. For security and privacy reasons, LC strongly recommends that the user should **not** modify these permissions to allow others access to their files.

Sensitive Processing

LC users who are processing sensitive data on an LC machine are responsible for establishing and maintaining adequate protection (file access controls, encryption, etc.) to protect their sensitive data. Sensitive unclassified information otherwise known as Unclassified Controlled Information (UCI) as it pertains to LC users is plain text or machine-encoded data that has relative sensitivity and requires mandatory protection because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect national or other DOE interests. Sensitive data types include, but are not limited to, Official Use Only (OUO) and Export Controlled Information (ECI). Unclassified Controlled Nuclear Information (UCNI) and Naval Nuclear Propulsion Information (NNPI) may not be processed on LC systems except for systems explicitly designated to contain or store that type of sensitive data. User-defined proprietary data is permitted at LC, but the owner may require the use of additional protection mechanisms. Additional information is available through LLNL's Office of Classification and Export Control.

Data Protection

Users are advised to take appropriate measures to protect information and applications. Computers and network systems are inherently insecure. It is each user's responsibility to ensure that adequate protective measures are used to transmit and secure data.

Foreign National (FN) Access

Principal Investigators are required to provide citizenship and names of any of their FN users. An F-2311 must be completed for all FNs requesting access to LC resources. Other required documents for FN access include a Computer Security Plan (CSP) and Program Justification for FN Computer Access. FNs from sensitive countries may be granted access with restricted privileges in order for DOE to comply with export controls and national security and non-proliferation restrictions. Access to restricted data is subject to DOE approval.

Altering Authorized Access

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

Waste, Fraud and Abuse

The DOE Unclassified Computer Security Program requires that DOE computers be protected from waste, fraud, and abuse. LC personnel and users are required to address, safeguard against and report misuse, abuse and criminal activities. LC is required to review the contents of unclassified computer files at unannounced intervals by means of random sampling.

Termination

Non-compliance with these Policies and Procedures or misuse of LC resources can lead to temporary or permanent disabling of accounts, loss of DOE allocations, administrative actions, civil liability, and criminal prosecution.

Additional Terms Applicable to COVID-19 High Performance Computing Consortium

Except as otherwise set forth in other written agreements with LLNS, any work relating to the COVID-19 pandemic using Livermore Computing resources is funded by DOE and therefore all research results and any inventions or works that arise therefrom shall be non-proprietary and publicly releasable, and User's research results must be published in open literature. To the extent not so published, the U.S. Government shall have for itself and those acting on its behalf a worldwide, non-exclusive, irrevocable, royalty-free license to exercise all rights under any inventions or works related to COVID-19 and produced using Livermore Computing resources.

Access to Livermore Computing resources for COVID-19 research includes use of LC-provided software that is routinely made available to all LC users (e.g., compilers, debuggers, etc.), subject to any third party licensing requirements or limitations, but does not include collaboration with LLNL researchers or scientists beyond technical support related to utilizing the LC resources, or use of any other proprietary software or intellectual property. Any such collaboration, additional services, or additional software/intellectual property use must be addressed in a separate written agreement.

NEITHER LAWRENCE LIVERMORE NATIONAL SECURITY, LLC (LLNS) NOR THE U.S. GOVERNMENT MAKE ANY EXPRESS OR IMPLIED WARRANTIES: (A) CONCERNING THE LIVERMORE COMPUTING RESOURCES, WHICH ARE PROVIDED "AS IS"; (B) CONCERNING USER'S RESEARCH OR ANY RESULTS OR INTELLECTUAL PROPERTY RESULTING THEREFROM; OR (C) THAT USER'S USE OF THE LIVERMORE COMPUTING RESOURCES WILL BE UNINTERRUPTED OR ERROR-FREE. WITHOUT LIMITING THE FOREGOING, ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES ARE DISCLAIMED BY LLNS AND THE U.S. GOVERNMENT, INCLUDING WITH RESPECT TO MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. NEITHER LLNS NOR THE U.S. GOVERNMENT SHALL BE LIABLE TO USER OR HIS OR HER EMPLOYER FOR ANY DAMAGES ATTRIBUTED TO USER'S USE OF THE LIVERMORE COMPUTING RESOURCES OR ANY RESULTS THEREFROM.

Sign electronically in the IdM account system.

Lawrence Livermore National Laboratory, PO Box 808 L-63, Livermore CA 94551 • Fax (925) 422-0592
Questions? Contact the LC Customer Service Group by phone at (925) 422-4531, Option 2 or send e-mail to lc-support@llnl.gov

Livermore Computing Policies and Procedures

Lawrence Livermore National Laboratory •PO Box 808, L-63 •Livermore CA 94551 •Fax (925) 422-0592

Acceptance of Terms of the Statement of Policies and Procedures

I have read the *LIVERMORE COMPUTING Policies and Procedures* and agree to abide by the requirements set forth in this document when using LIVERMORE COMPUTING/LAWRENCE LIVERMORE NATIONAL LABORATORY computing resources. If I am accessing and using the LC computing resources in connection with my employment, I represent that I am authorized by my employer to agree to these Policies and Procedures and that they do not conflict with any obligations I may owe to my employer. This agreement may be enforced by Lawrence Livermore National Security, LLC, or by DOE, or by any successor contractor that manages Lawrence Livermore National Laboratory. I acknowledge awareness of the following Computer Security Warning, which applies to all Federal computer systems I access and I consent to the terms and conditions of use as stated below:

This is a Federal computer system and is the property of the United States Government. It is for authorized use only. **Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.** Any or all uses of this system and all files on the system may be intercepted, monitored, recorded, copied, audited, inspected and disclosed to authorized site personnel, Department of Energy personnel, law enforcement personnel, and officials of other agencies, both domestic and foreign. **By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel.**

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.
LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

Last Name	First Name	Middle Initial
Unclassified E-mail	Citizenship (if not U.S., include VTS/Fast Track numbers)	
User Signature	Date	
User's Employer's Name		

LC Customer Service Group
Lawrence Livermore National Laboratory, PO Box 808 L-63, Livermore CA 94551 • Fax (925) 422-0592
Questions? Contact the LC Customer Service Group by phone at (925) 422-4531, Option 2 or send e-mail to lc-support@llnl.gov