

LAWRENCE LIVERMORE NATIONAL LABORATORY

ACCESS TO LLNL COMPUTER RESOURCES PROVISIONS

The following provisions shall apply if any Subcontractor personnel, at any tier, will have access to any LLNL computer resources either on-site or remotely. As used herein, the term "Subcontractor" shall also mean "Seller" and the term "Subcontract" shall also mean "Agreement" or "Purchase Order."

- A. The performance of this Subcontract may require Subcontractor personnel (including lower-tier subcontractor personnel) to use or connect with LLNL computer resources (i.e., computers or computer networks). Any such access and use shall comply with Department of Energy Acquisition Regulation (DEAR) 952.204-77, *Computer Security* (AUG 2006) which is hereby incorporated by reference into this Subcontract; and shall be in accordance with and subject to LLNL Cyber Security Program (LLNL CSP) requirements, including the following:
1. Approval to access specific LLNL computer resources shall be obtained from the appropriate LLNL Organization Information Systems Security Officer (OISSO), through the LLNS Technical Representative. Subcontractor personnel must meet training and other requirements before being granted access to LLNL computer resources.
 2. Access to LLNL computer resources by Subcontractor personnel is only permitted as required to perform the work authorized under this Subcontract. Classified computer resources or information shall not be accessed or attempted to be accessed without specific written authorization from the LLNL CSP, through the LLNS Technical Representative. Personal and non-work-related use of LLNL computer resources by Subcontractor personnel is prohibited.
 3. Only Subcontractor personnel who are U.S. citizens may access or use LLNL computer resources, unless specific written authorization is granted for each non-U.S. citizen by the LLNL CSP, through the LLNS Technical Representative.
 4. Only the approved Virtual Private Network (VPN) or High Performance Computing (HPC) Enclave access methods shall be used to remotely access unclassified LLNL resources.
 5. All software used by Subcontractor personnel on LLNL computer resources must be appropriately acquired and used according to the applicable licensing agreements.
 6. All information or data furnished by LLNS or obtained from or developed on a LLNL computer resource by Subcontractor personnel shall be treated as confidential and protected by the Subcontractor to prevent disclosure to any persons other than those authorized by LLNS.

7. Computer passwords used by Subcontractor personnel for LLNL computer resources shall comply with the applicable LLNL rules and policies and be protected to prevent disclosure to other persons. If a computer password is disclosed, or disclosure is suspected, the Subcontractor shall immediately notify the LLNS Technical Representative and arrange for replacement of the password.
 8. Non-LLNL electronic devices and computers are prohibited from connecting to LLNL networks or equipment except for the Guest network without the written approval of the LLNS Technical Representative and the LLNL Organizational Information System Security Officer (OISSO). Restrictions apply for the use of non-LLNL electronic devices and computers in Limited Areas buildings.
- B. These requirements shall be applicable whether such access is at the LLNL, at the Subcontractor's facility, or elsewhere; and shall be applicable to lower-tier subcontractors and their personnel whose work requires access to LLNL computer resources. The Subcontractor shall report any suspected or actual computer security incident as soon as possible to the LLNS Technical Representative and the Security Operations Center Hotline at either 925-422-4655 (M-F from 8:00AM – 5:00PM), 925-456-4759 (after business hours), or send email to imt@llnl.gov.
- C. LLNS may monitor the use of LLNL computer resources by network operating software, reviewing the contents of all LLNL computer resources and any computers used to access LLNL computer resources, and other appropriate means.
- D. If the Subcontractor does not comply with the provisions of this article, LLNS may withdraw the Subcontractor's access to LLNL computer resources. Misuse of LLNL computer resources may be a violation of law and could result in appropriate action, including termination for default and/or criminal prosecution.
- E. In accordance with National Nuclear Security Administration (NNSA) Supplemental Directive 206.2 (once implemented), when the Subcontractor or its lower-tier subcontractor personnel require on-site and/or logical access (i.e., remote access to information technology systems) to LLNL for more than 179 days or a combination thereof (cumulative in a calendar year), its personnel must be processed for Personal Identity Verification (PIV) by LLNS. If the individual subject to the PIV fails to provide his or her verifiable identity or is found unsuitable, LLNS will deny all access (physical or logical) to the individual. The Subcontractor is responsible for immediately removing the individual from the worksite at no additional cost to LLNS.

(END OF PROVISIONS)